HP ProLiant BL p-Class GbE2 Interconnect Switch

Browser-based Interface Reference Guide

Part number: 331401-007

Seventh edition: March 2007

Legal notices

Part number: 331401-007

Seventh edition: March 2007

Contents

Configuring the switch

Getting started

Introduction

The HP ProLiant BL p-Class GbE2 Interconnect Switch software lets you use your Web browser to access GbE2 Interconnect Switch information and statistics and perform switch configuration via the Internet.

This guide provides an overview of how to access and use the GbE2 Interconnect Switch browser-based interface (BBI).

This chapter briefly describes the software features and requirements for the HP ProLiant BL p-Class GbE2 Interconnect Switch browser-based interface (BBI) and explains how to access the BBI start page.

Additional references

Additional information about installing and configuring the GbE2 Interconnect Switch is available in the following guides, which are available at **http://www.hp.com/support**.

- *HP ProLiant BL p-Class GbE2 Interconnect Switch User Guide*
- *HP ProLiant BL p-Class GbE2 Interconnect Switch Application Guide*
- *HP ProLiant BL p-Class GbE2 Interconnect Switch Command Reference Guide*
- *HP ProLiant BL p-Class C-GbE2 Interconnect Kit Quick Setup Instructions*
- *HP ProLiant BL p-Class F-GbE2 Interconnect Kit Quick Setup Instructions*
- *HP BladeSystem p-Class SAN Connectivity Kit Quick Setup Instructions*

Features

The network administrator can access all switch configuration and monitoring functions through the BBI, a Web-based switch management interface. The BBI has the following features:

- Most of the same configuration and monitoring functions as the command line interface
- Intuitive and easy-to-use interface structure
- Nothing to install; the BBI is part of the switch software
- Two default levels of password protection
- Can be upgraded as future software releases are available

Requirements

To use the browser-based interface, you need the following:

- HP ProLiant BL p-Class GbE2 Interconnect Switch
- Installed HP ProLiant BL p-Class GbE2 Interconnect Switch software
- PC or workstation with network access to the switch
- Frame-capable Web-browser software, such as the following:
  - Netscape Navigator 4.7x or higher
  - Internet Explorer 6.0x or higher
- JavaScript enabled in your Web browser

GbE2 Interconnect Switch setup

Before you can access the BBI, minimal configuration is required on the switch.

Configuring IP interfaces

At least one IP interface must be configured on the switch. This is usually done from the command line interface during first-time switch set up. Each IP interface address provides a point of access for HP ProLiant BL p-Class GbE2 Interconnect Switch management.

For more information about configuring an IP interface for management access, see the "Using the command line interface" section in the "Accessing the GbE2 Interconnect Switch" chapter of the *HP ProLiant BL p-Class GbE2 Interconnect Switch Application Guide*.

Enabling or disabling BBI access

By default, BBI access is enabled. If you need to disable or re-enable access, use the following command from the command line interface:

```
>> Main# /cfg/sys/access/http <disable|enable (or just d|e)>
```

By default, secure BBI access is disabled. If you need to enable access, use the following command from the command line interface:

```
>> Main# /cfg/sys/access/https/https <disable|enable (or just d|e)>
```

The default TCP port to use for BBI access is port 80. To change the port number, use the following command:

```
>> Main# /cfg/sys/access/wport <TCP port number>
```

For more information on accessing and configuring the GbE2 Interconnect Switch through the command line interface, refer to the *HP ProLiant BL p-Class GbE2 Interconnect Switch Command Reference Guide*.

Web browser setup

Most modern Web browsers work with frames and JavaScript by default, and require no additional set up. However, you should check your Web browser's features and configuration to make sure frames and JavaScript are enabled.

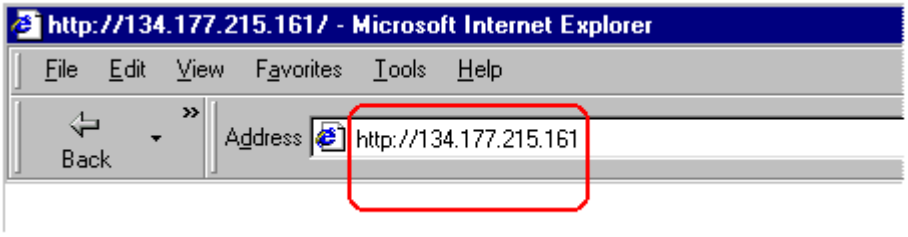
NOTE: JavaScript is not the same as Java™. Make sure that JavaScript is enabled in your Web browser.

Starting the BBI

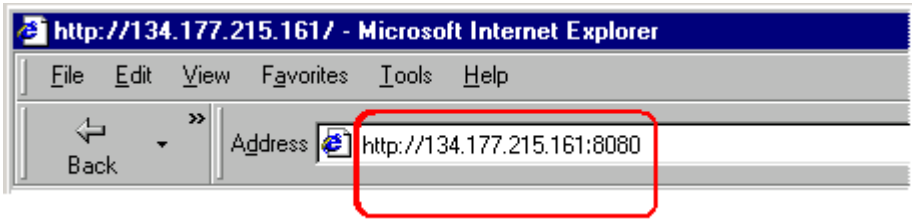
When the GbE2 Interconnect Switch and browser setup is complete, follow these steps to launch the BBI:

1. Start your Web browser.
2. Enter the GbE2 Interconnect Switch IP interface address in the Web browser Uniform Resource Locator (URL) field.

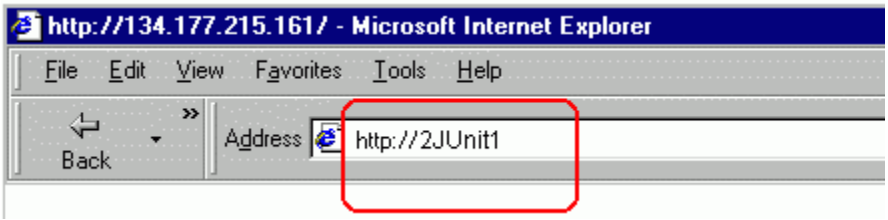
   For example, if the GbE2 Interconnect Switch IP interface has a network IP address of 134.177.215.131. Using Internet Explorer, you could enter the following (for secure BBI access, use https://).



   If you do not use the default TCP port number (80) for BBI access, you can include the port number when you enter the IP address:

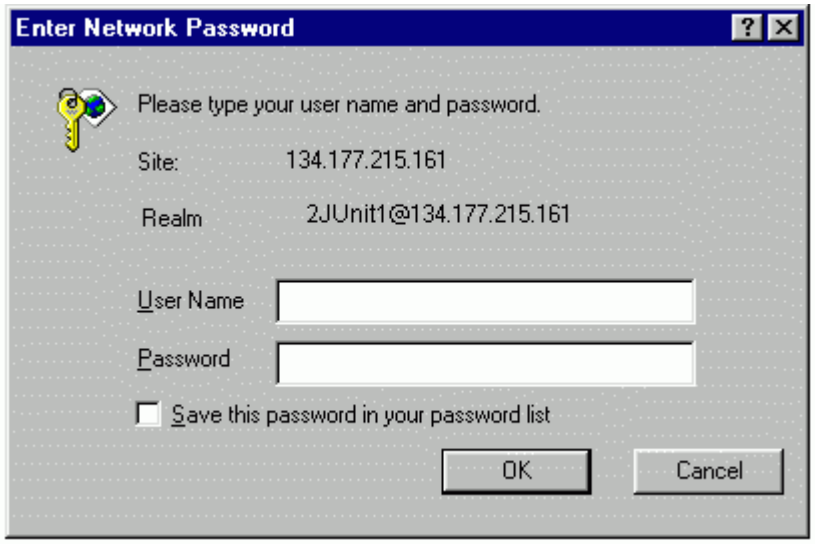


If the GbE2 Interconnect Switch IP interface address has a name on your local domain name server, you can enter the name instead. Using Internet Explorer, you can enter the following:



3. Log in to the GbE2 Interconnect Switch.

   If your GbE2 Interconnect Switch and browser are properly configured, you will be asked to enter a password.

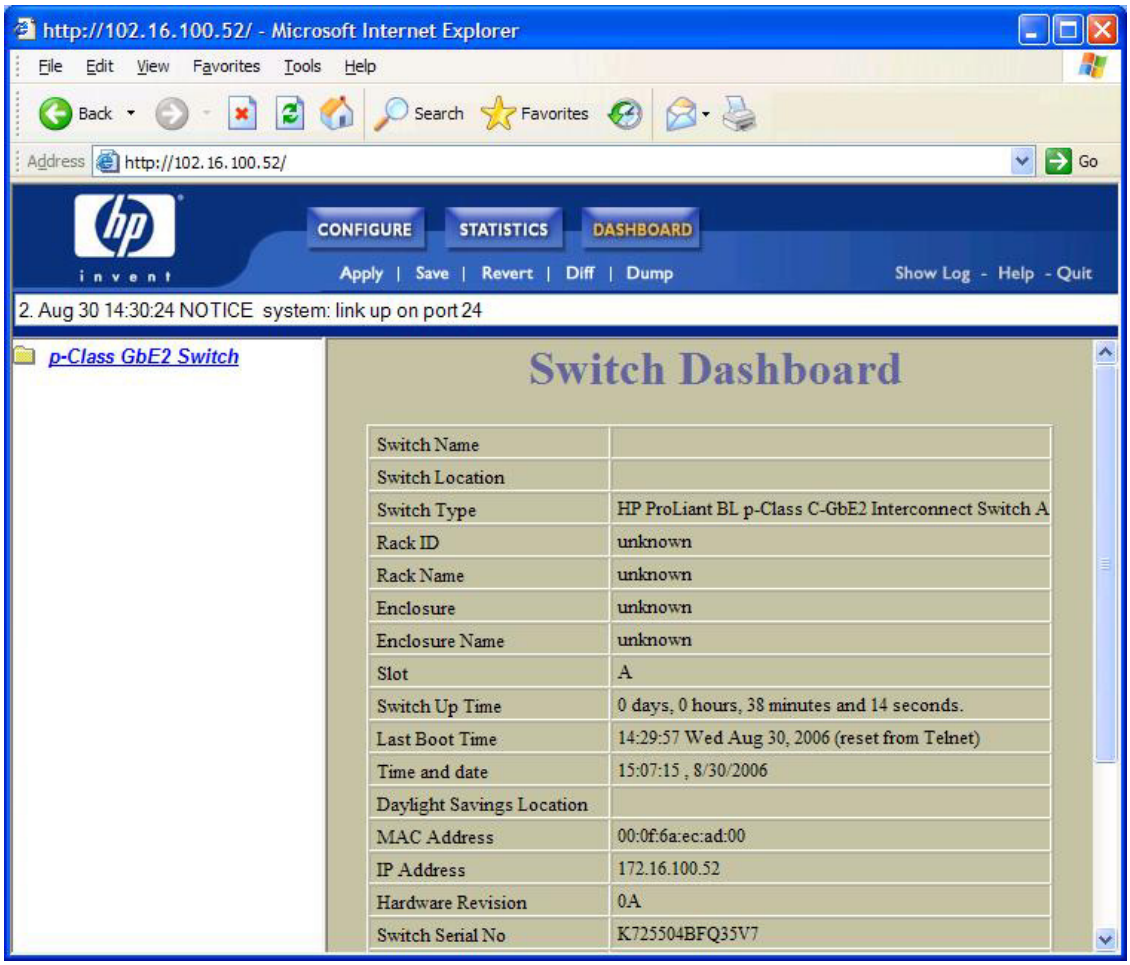


   Enter the account name and password for the switch.

   For more password information, see the *HP ProLiant BL p-Class GbE2 Interconnect Switch Command Reference Guide*.

4. Allow the BBI Dashboard page to load.

   When the proper account name and password combination is entered, the BBI Dashboard page is displayed in the browser viewing area.



NOTE: There may be a slight delay while the Dashboard page is initializing. You should not stop the browser while loading is in progress. When loading is complete, a folder icon with the GbE2 Interconnect Switch IP address displays in the left-hand BBI window. Click this folder and a tree of folders displays.

Browser-based interface basics

Introduction

Once you are properly logged in, the GbE2 Interconnect Switch BBI displays in the Web browser-viewing window.

There are three main regions on the screen.

- The toolbar is used for selecting the context for your actions in the other windows.
- The navigation window is used for selecting particular items or features to act upon.
- The forms window is used for viewing or altering GbE2 Interconnect Switch information.

Toolbar

The toolbar contains buttons and commands used to access and execute GbE2 Interconnect Switch functions.

Context buttons

The toolbar is used for setting the context for your actions in the application. There are three context buttons:

Table 1 Context buttons

Button	Description
Configure	When selected, you can access and alter the GbE2 Interconnect Switch configuration forms. Select an item in the navigation window to display the desired configuration form in the forms window. **Note:** This context is only available when you are logged in as an administrator.
Statistics	When selected, you can view information about GbE2 Interconnect Switch performance. Select an item in the navigation window to display the desired statistics in the forms window.
Dashboard	This context button is selected by default when the BBI is first activated. When selected, basic GbE2 Interconnect Switch information and status can be viewed in the forms window. Select an item in the navigation window to display the desired dashboard information in the forms window.

First click a context button, and then click an item in the navigation window. When a context button is selected, the button is highlighted as a reminder of the current context mode.

Commands

The following general commands are available on the toolbar:

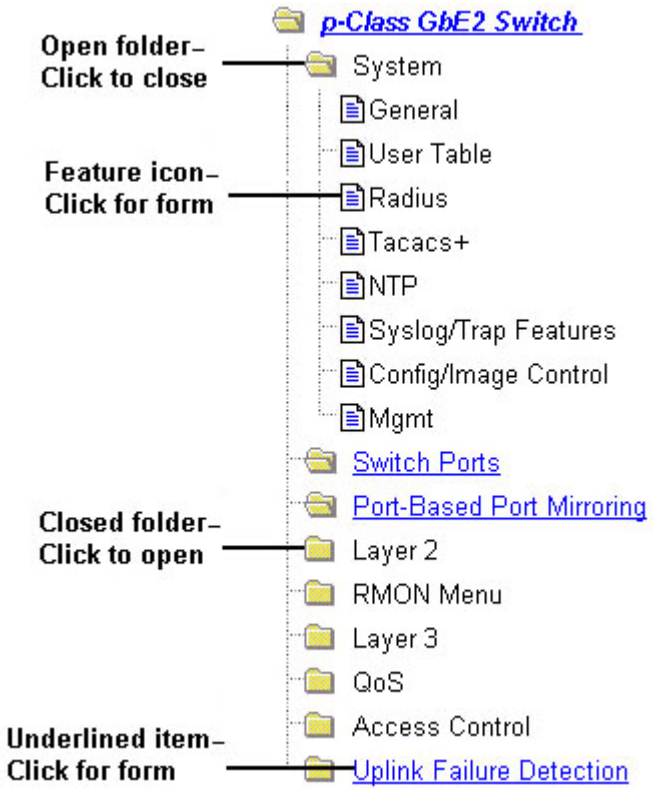
Table 2 Toolbar commands

Command	Description
Apply	Pending configuration changes do not take effect until you select the **Apply** command. Once applied, all changes (except enabling/disabling Spanning Tree Protocol) take effect on the GbE2 Interconnect Switch immediately. If you do not save the changes, however, they will be lost the next time the switch is rebooted.
Save	Writes applied configuration changes to non-volatile flash memory on the GbE2 Interconnect Switch (with the option of not overlaying the current backup).
Revert	Removes pending configuration changes between **Apply** commands. Use this command to restore configuration parameters set since last **Apply** command.
Diff	Shows any pending configuration changes.
Dump	Writes current GbE2 Interconnect Switch configuration to the screen. Configuration information is displayed with parameters that have been changed from default values.
Show Log	Opens a new Web-browser window for displaying the 100 most recent GbE2 Interconnect Switch log messages. Close the log browser when finished.
Help	Opens a new Web-browser window for displaying the basic online help information. Close the help browser when finished.
Quit	Logs off the GbE2 Interconnect Switch and exits the BBI.

Navigation window

The navigation window is used for selecting a particular GbE2 Interconnect Switch feature to act upon. Status, statistics, or configuration forms for the selected item will display in the forms window, depending on the context chosen on the toolbar.

The navigation window contains a tree of folders, subfolders, and feature icons.



Click any closed folder to open it and reveal its contents. Click any open folder to close it. Click any feature icon to load the appropriate status, statistics, or configuration form in the forms window.

Some folders also have forms. If the name of a folder is underlined, click the name to display the appropriate form.

Forms window

When a feature icon is selected on the navigation window, a status, statistics, or configuration form is displayed in the forms window. The exact nature of the form depends on the current context selected on the toolbar, as well as the type of information available. Not all feature icons have forms for all contexts.

Some forms display GbE2 Interconnect Switch information such as settings, status, or statistics. Others allow you to make configuration changes to GbE2 Interconnect Switch parameters.

NOTE: Some items display blank forms, depending on the context. A blank form indicates that no information or actions are available in that context.

Dashboard

Introduction

The GbE2 Interconnect Switch BBI can be used to view the present settings and operating status of a variety of GbE2 Interconnect Switch features. Most of the same information available through the switch's command line interface is present on the dashboard forms.

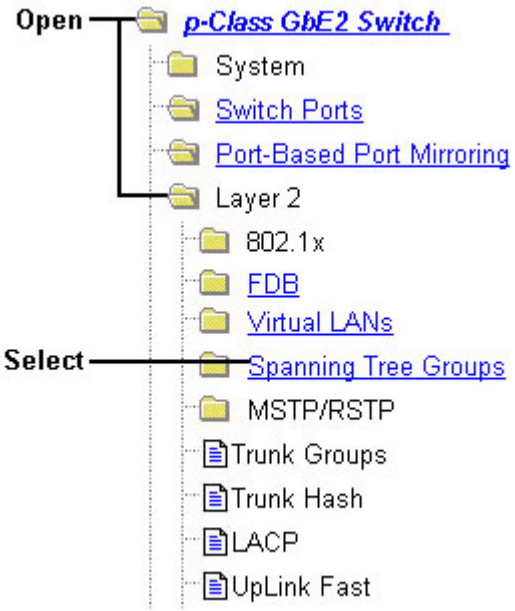
The following provides a basic outline for viewing the dashboard forms. You should first be familiar with configuration as covered in the *HP ProLiant BL p-Class GbE2 Interconnect Switch Command Reference Guide*.

Steps for displaying dashboards

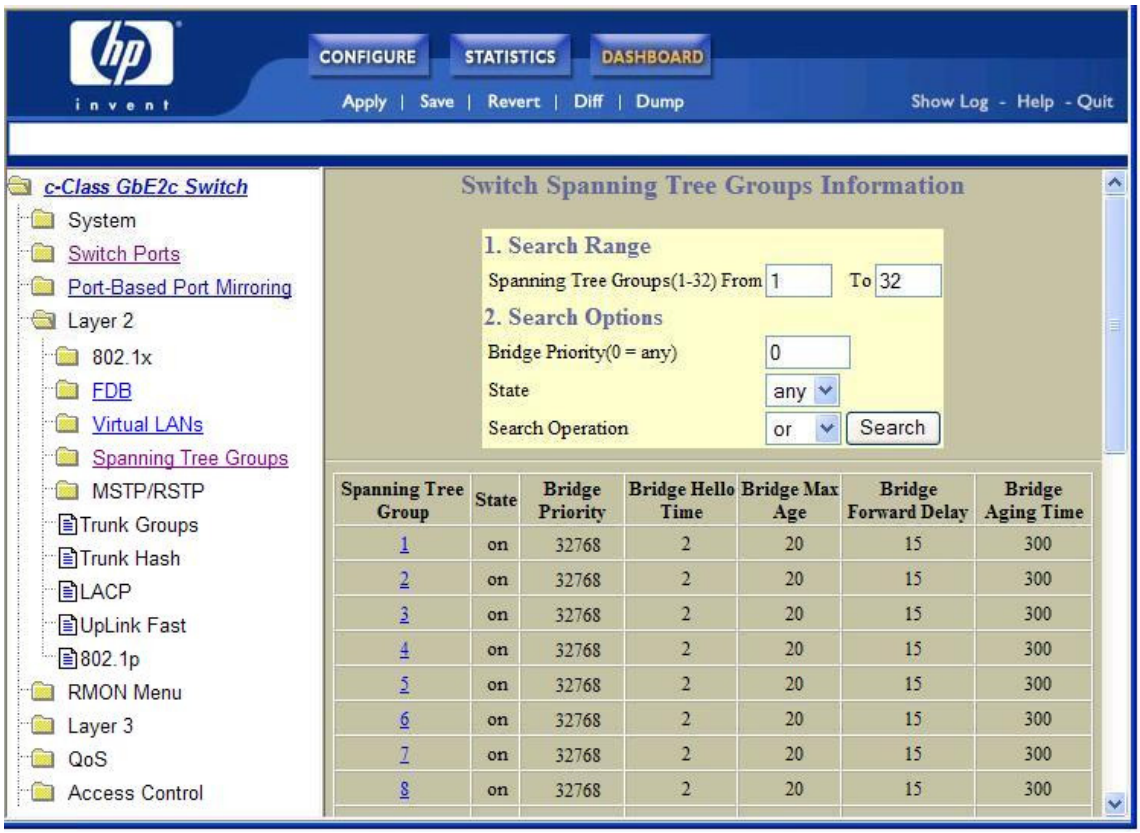
Follow these basic steps for viewing switch dashboard forms.

1. Select the **Dashboard** context button in the BBI toolbar.

2. Select a feature icon in the navigation window. For example, select **Spanning Tree Groups**:



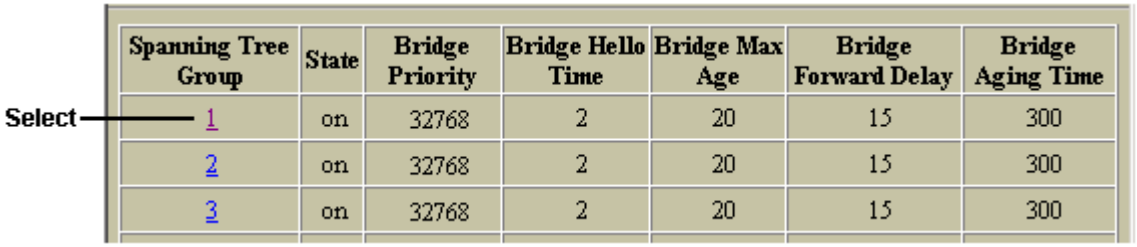
3. View information shown in the forms window.



Spanning Tree Group	State	Bridge Priority	Bridge Hello Time	Bridge Max Age	Bridge Forward Delay	Bridge Aging Time
1	on	32768	2	20	15	300
2	on	32768	2	20	15	300
3	on	32768	2	20	15	300
4	on	32768	2	20	15	300
5	on	32768	2	20	15	300
6	on	32768	2	20	15	300
7	on	32768	2	20	15	300
8	on	32768	2	20	15	300

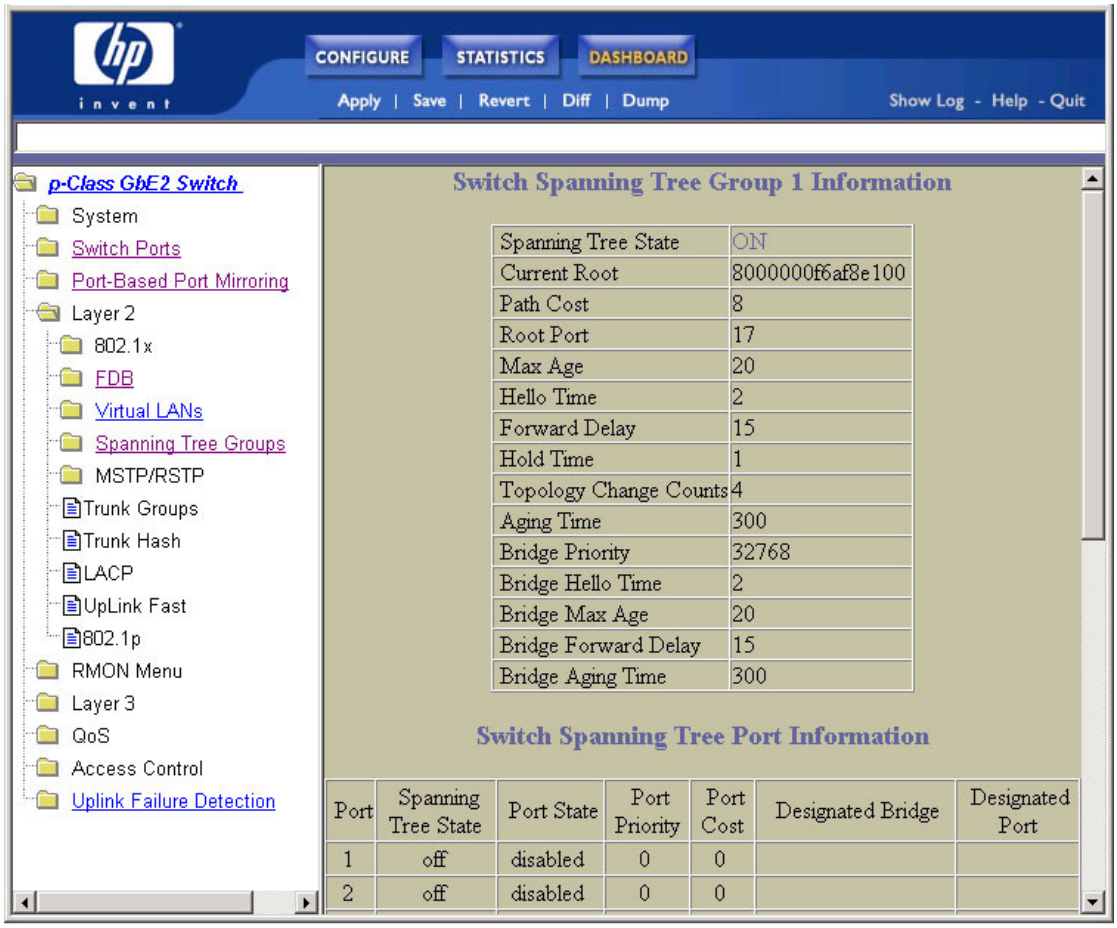
NOTE: Items that load other forms when selected are underlined.

4. Select an underlined item to view details or perform actions.



Spanning Tree Group	State	Bridge Priority	Bridge Hello Time	Bridge Max Age	Bridge Forward Delay	Bridge Aging Time
1	on	32768	2	20	15	300
2	on	32768	2	20	15	300
3	on	32768	2	20	15	300

In this example, click a Spanning Tree Group number to view detailed information about the group (shown in form below).



Switch Dashboard

To display the following form, select **System > General**. This is the default form for the switch.

Switch Dashboard

Switch Name	
Switch Location	
Switch Type	HP ProLiant BL p-Class C-GbE2 Interconnect Switch A
Rack ID	unknown
Rack Name	unknown
Enclosure	unknown
Enclosure Name	unknown
Slot	A
Switch Up Time	0 days, 1 hour, 13 minutes and 52 seconds.
Last Boot Time	14:29:57 Wed Aug 30, 2006 (reset from Telnet)
Time and date	15:43:14 , 8/30/2006
Daylight Savings Location	
MAC Address	00:0f:6a:ec:ad:00
IP Address	172.16.100.52
Hardware Revision	0A
Switch Serial No	K725504BFQ35V7
Hardware Part No	336181-001
HW Spare Part No	321148-001
Interconnect Module Part No	283192-B21
Interconnect Spare Part No	321147-001
OctalFC Module Part No	Not Present
OctalFC Spare Part No	Not Present
Software Rev	3.1.0 (FLASH image1)
Banner	

The following table describes the Switch Dashboard controls:

Table 3 Switch Dashboard controls

Control	Description
Switch Name	Displays the name of the switch, as entered in Configuration > Switch > General (SNMP).
Switch Location	Displays the location of the switch, as entered in Configuration > Switch > General (SNMP).
Switch Type	Displays the type of switch.
Rack ID	Displays the serial number of the chassis in which the switch resides.
Rack Name	Displays the name of the chassis in which the switch resides.
Enclosure	Displays the serial number of the enclosure (or “bay”) in which the switch resides.
Enclosure Name	Displays the name of number of the enclosure (or “bay”) in which the switch resides.
Slot	Displays the slot in which the switch resides.
Switch Up Time	Displays the amount of time the switch has been running.
Last Boot Time	Displays the date and time of last switch boot.
Time and Date	Displays the current time and date settings on the switch.
Daylight Savings Location	Displays the time zone where the switch resides. You are prompted to select your location (continent, country, region) by the timezone wizard. Once a region is selected, the switch updates the time to reflect local changes to Daylight Savings Time, etc.
MAC Address	Displays the MAC Address of the switch management processor.
IP Address	Displays the IP address of IP Interface 1.
Hardware Revision	Displays the hardware revision number of the switch.
Switch Serial No	Displays the serial number of the switch.
Hardware Part No	Displays the part number of the switch hardware.
HW Spare Part No	Displays the part number of spare switch hardware.
Interconnect Module Part No	Displays the part number of the interconnect module, if applicable.
Interconnect Spare Part No	Displays the part number of the spare interconnect module, if applicable.
OctalFC Module Part No	Displays the part number of the OctalFC Module, if applicable.
OctalFC Spare Part No	Displays the part number of the spare OctalFC module, if applicable.
Software Rev	Displays the software revision number.
Banner	Displays the login banner text. When a user or administrator logs into the switch, the login banner is displayed. It is also displayed as part of the output from the `/info/sys/gen` command.

User Access Dashboard

To display the following form, select **System > User Table**.

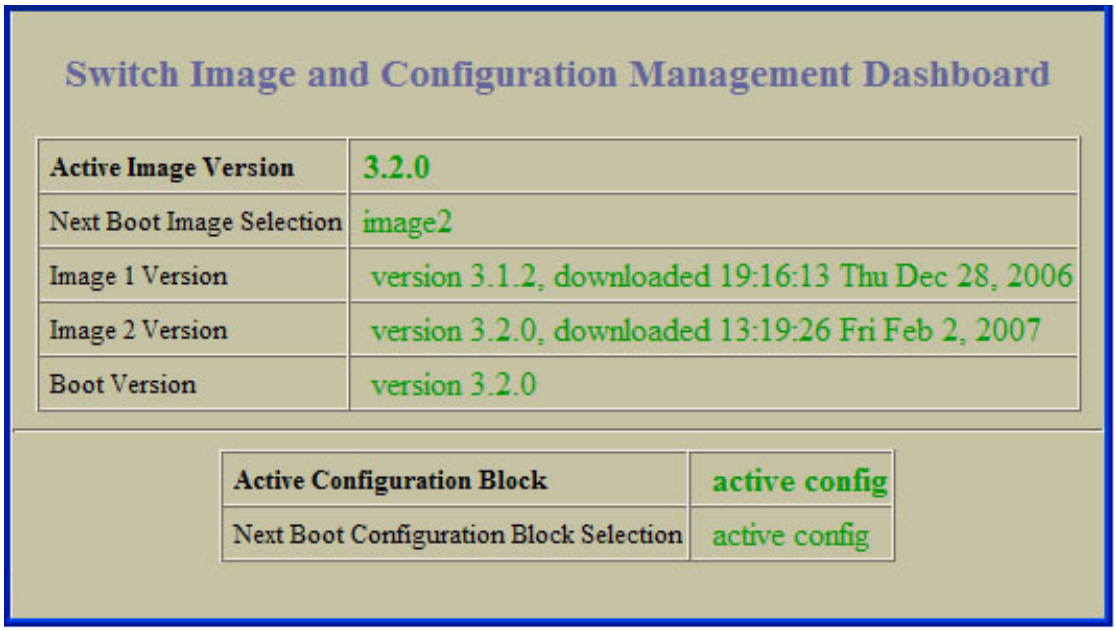
The following table describes the User Access Dashboard controls:

Table 4 User Access Dashboard controls

Control	Description
User ID	Displays the numeric identifier for the user
User Name	Displays the name of the user.
COS	Displays the Class of Service level for the user.
Password	Indicates whether a valid password is defined for the user.
Status	Displays whether the user is **enabled** or **disabled**.
Login	Displays the login status of the user (online or offline).

Switch Image and Configuration Management Dashboard

To display the following form, select **System > Config/Image Control**.



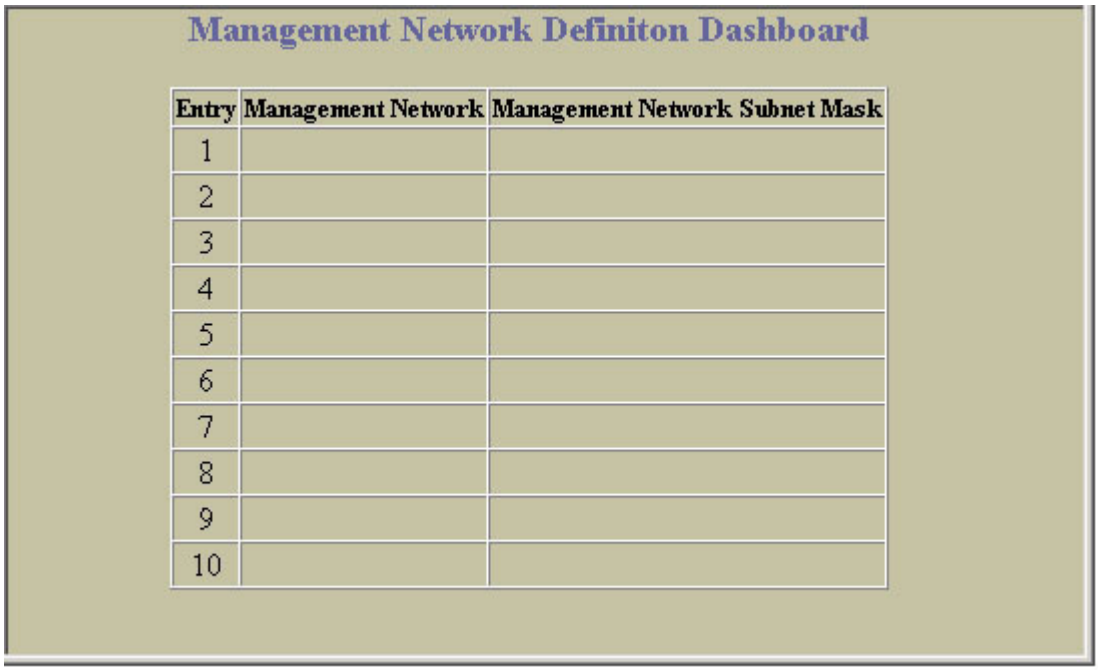
The following table describes the Switch Image and Configuration Dashboard controls:

Table 5 Switch Image and Configuration Dashboard controls

Control	Description
Active Image Version	Displays the number of the active software image.
Next Boot Image Selection	Displays which software image (image1 or image2) will be loaded into switch memory for the next reboot.
Image 1 Version	Displays information about the current Image 1 software.
Image 2 Version	Displays information about the current Image 2 software.
Boot Version	Displays the version number of the current Boot software.
Active Configuration Block	Defines which configuration block is selected for the currently running session.
Next Boot Configuration Block Selection	Allows the user to select the configuration block to be loaded upon the next reboot.

Management Network Definition Dashboard

To display the following form, select **System > Mgmt**.



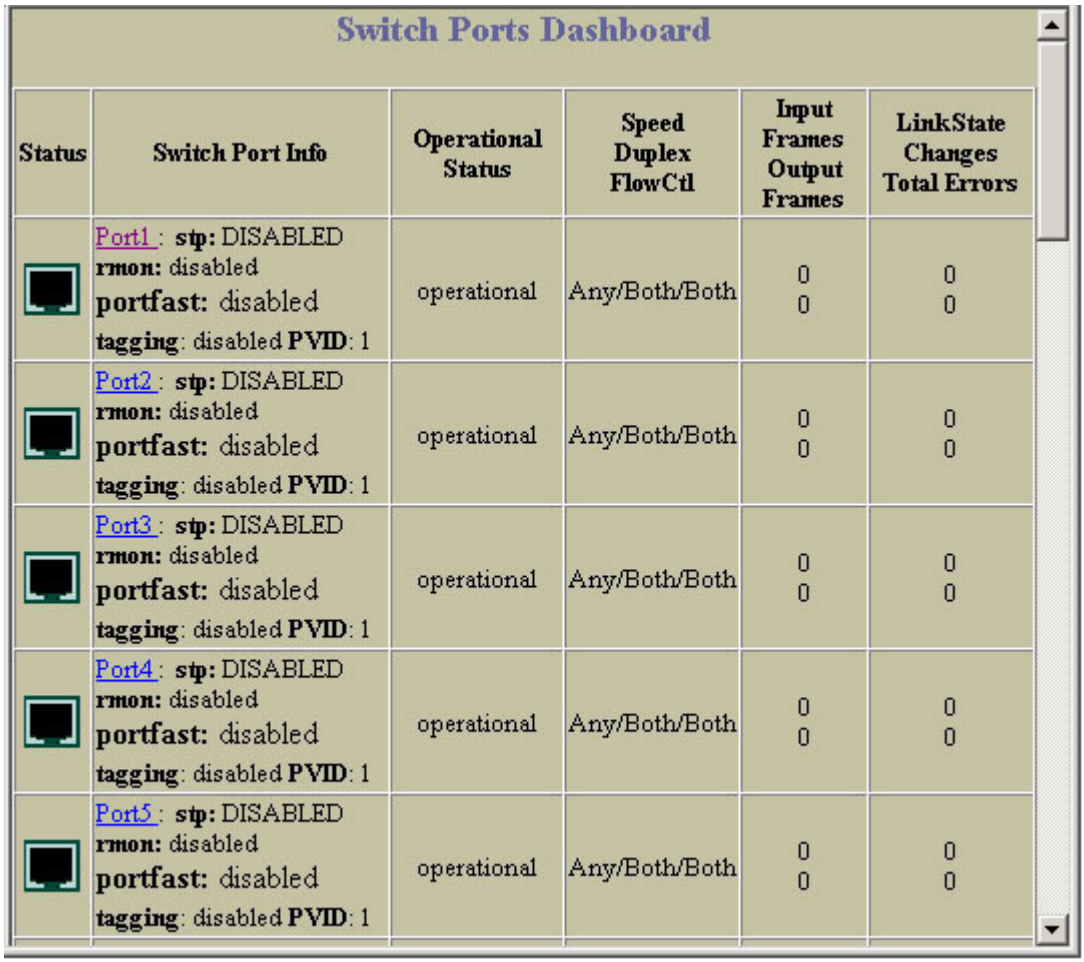
The following table describes the Management Network Definition Dashboard controls:

Table 6 Management Network Definition Dashboard controls

Control	Description
Entry	Displays the entry number for each management network.
Management Network	Displays the IP address of the management network.
Management Network Subnet Mask	Displays the subnet mask of the management network.

Switch Ports Dashboard

To display the following form, select **Switch Ports** (click the underlined text, not the folder).



Switch Ports Dashboard

Status	Switch Port Info	Operational Status	Speed Duplex FlowCtl	Input Frames Output Frames	LinkState Changes Total Errors
	Port1 : **stp:** DISABLED **rmon:** disabled **portfast:** disabled **tagging**: disabled **PVID**: 1	operational	Any/Both/Both	0 0	0 0
	Port2 : **stp:** DISABLED **rmon:** disabled **portfast:** disabled **tagging**: disabled **PVID**: 1	operational	Any/Both/Both	0 0	0 0
	Port3 : **stp:** DISABLED **rmon:** disabled **portfast:** disabled **tagging**: disabled **PVID**: 1	operational	Any/Both/Both	0 0	0 0
	Port4 : **stp:** DISABLED **rmon:** disabled **portfast:** disabled **tagging**: disabled **PVID**: 1	operational	Any/Both/Both	0 0	0 0
	Port5 : **stp:** DISABLED **rmon:** disabled **portfast:** disabled **tagging**: disabled **PVID**: 1	operational	Any/Both/Both	0 0	0 0

The following table describes the Switch Ports Dashboard controls:

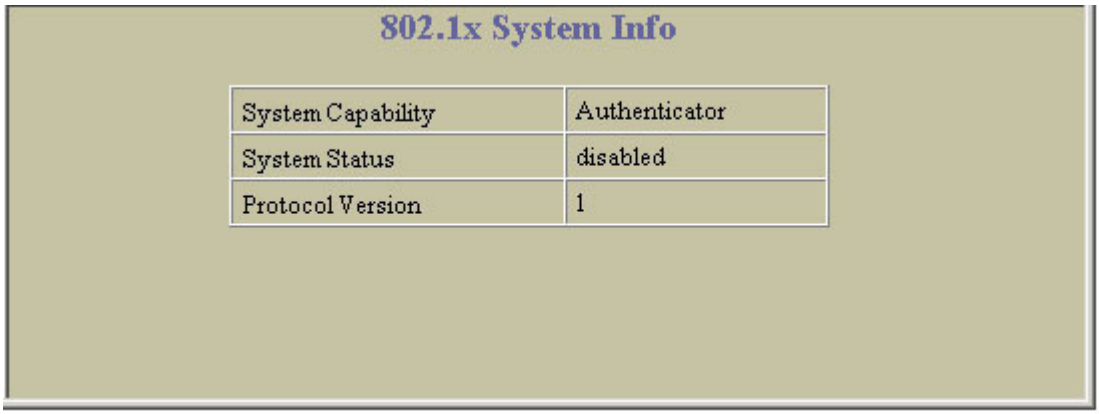
Table 7 Switch Ports Dashboard controls

Control	Description
Status	Shows if the port is enabled (green) or disabled (black).
Switch Port Info	Summarizes the following port information: **STP**: Shows if the port has Spanning Tree Protocol **enabled** or **disabled**. **rmon**: Shows if RMON is **enabled** or **disabled**. **portfast**: Shows if Port Fast Forwarding is **enabled** or **disabled**. **tagging**: Shows if this port has VLAN Tagging **enabled** or **disabled**. **PVID**: VLAN ID of any VLAN(s) to which this port is a member.
Operational Status	Displays the operational status of the port.
Speed/Duplex/Flow Ctl	Displays parameters for the port link.
Input Frames/Output Frames	Displays the number of frames that have been received by this port (Input Frames) and the number of frames that have been transmitted by this port (Output Frames).
Link State Changes/Total Errors	Displays the total number of link state changes for this port and the total number of errors logged by this port.

For more information, select a port number to display detailed statistics for that port.

802.1x System Information

To display the following form, select **Layer 2 > 802.1x > General**.



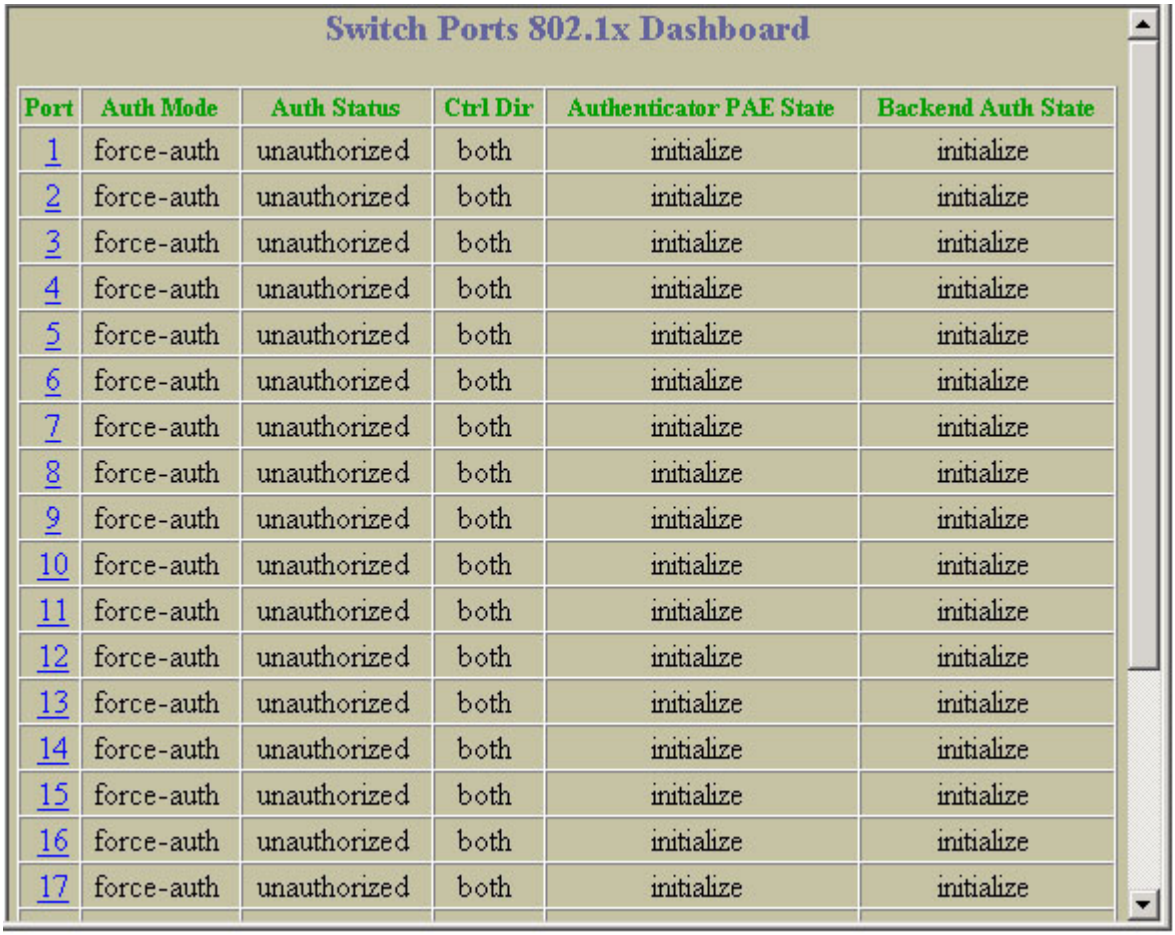
The following table describes the 802.1x system information fields:

Table 8 802.1x System information

Control	Description
System Capability	Displays the capability of the GbE2 Interconnect Switch as an 802.1x Authenticator. It cannot be used as an Authentication Server or a Supplicant.
System Status	Displays the current state (**enabled** or **disabled**) of 802.1x access control.
Protocol Version	Displays the 802.1x protocol version number.

Switch Ports 802.1x Dashboard

To display the following form, select **Layer 2 > 802.1x > Switch Ports**.



Switch Ports 802.1x Dashboard

Port	Auth Mode	Auth Status	Ctrl Dir	Authenticator PAE State	Backend Auth State
1	force-auth	unauthorized	both	initialize	initialize
2	force-auth	unauthorized	both	initialize	initialize
3	force-auth	unauthorized	both	initialize	initialize
4	force-auth	unauthorized	both	initialize	initialize
5	force-auth	unauthorized	both	initialize	initialize
6	force-auth	unauthorized	both	initialize	initialize
7	force-auth	unauthorized	both	initialize	initialize
8	force-auth	unauthorized	both	initialize	initialize
9	force-auth	unauthorized	both	initialize	initialize
10	force-auth	unauthorized	both	initialize	initialize
11	force-auth	unauthorized	both	initialize	initialize
12	force-auth	unauthorized	both	initialize	initialize
13	force-auth	unauthorized	both	initialize	initialize
14	force-auth	unauthorized	both	initialize	initialize
15	force-auth	unauthorized	both	initialize	initialize
16	force-auth	unauthorized	both	initialize	initialize
17	force-auth	unauthorized	both	initialize	initialize

The following table describes the Switch Ports 802.1x Dashboard fields:

Table 9 Switch Ports 802.1x Dashboard

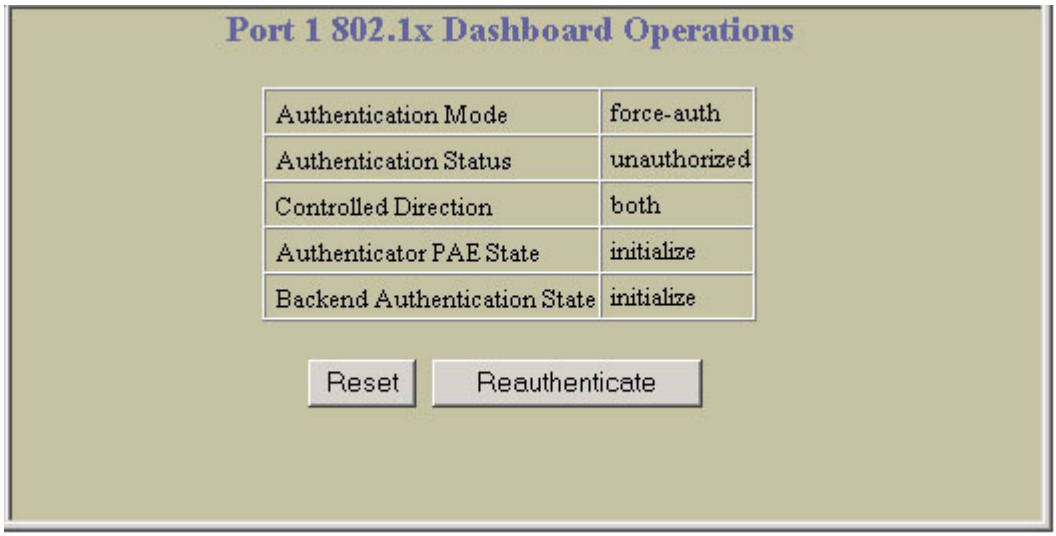
Field	Description
Port	Displays each port's name.
Auth Mode	Displays the Access Control authorization mode for the port. The Authorization mode can be one of the following: • force-unauth • auto • force-auth
Auth Status	Displays the current authorization status of the port, either authorized or unauthorized.
Ctrl Dir	Displays the controlled direction for the port, as follows: • **both:** indicates that control is exerted over both incoming and outgoing traffic through the controlled port. • **In:** indicates that control is exerted only over incoming traffic through the controlled port.
Authenticator PAE State	Displays the Authenticator Port Access Entity State. The PAE state can be one of the following: • initialize • disconnected • connecting • authenticating • authenticated • aborting • held • forceAuth

Table 9 Switch Ports 802.1x Dashboard

Field	Description
Backend Auth State	Displays the Backend Authentication State. The Backend Authentication state can be one of the following: • request • response • success • fail • timeout • idle

Port 802.1x Dashboard Operations

To display the following form, go to the Switch Ports 802.1x dashboard. Select a port number.



The following table describes the Port 802.1x Dashboard controls:

Table 10 Port 802.1x Dashboard controls

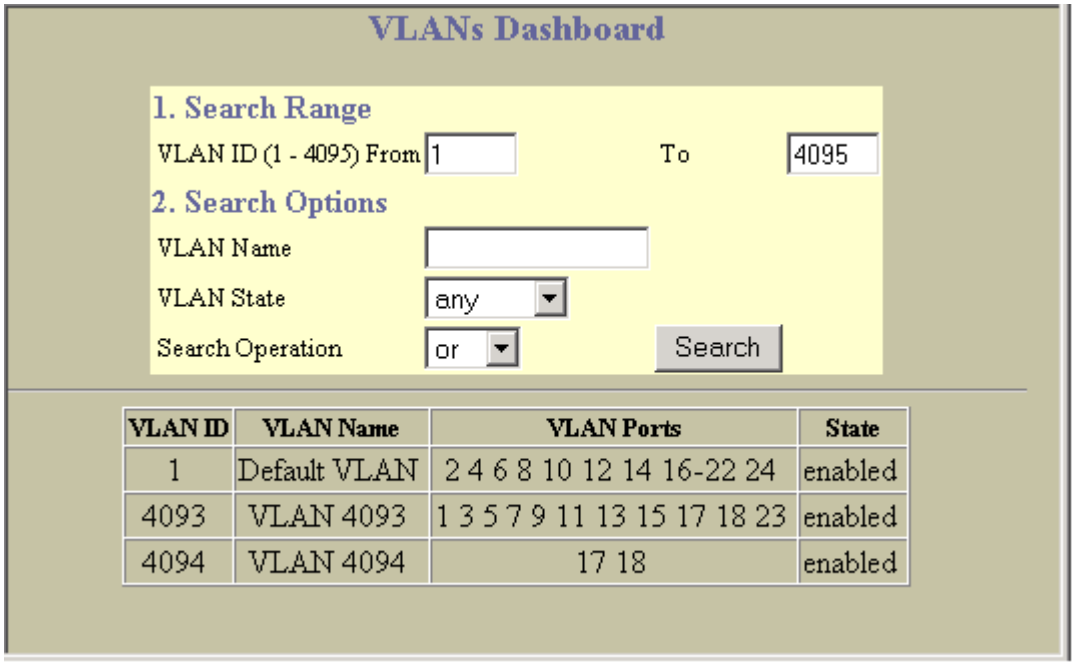
Control	Description
Authentication Mode	Displays the Access Control authorization mode for the port. The Authorization mode can be one of the following: • force-unauth • auto • force-auth
Authentication Status	Displays the current authorization status of the port, either authorized or unauthorized.
Controlled Direction	Displays the controlled direction for the port, as follows: • **both:** indicates that control is exerted over both incoming and outgoing traffic through the controlled port. • **In:** indicates that control is exerted only over incoming traffic through the controlled port.
Authenticator PAE State	Displays the Authenticator Port Access Entity State. The PAE state can be one of the following: • initialize • disconnected • connecting • authenticating • authenticated • aborting • held • forceAuth

Table 10 Port 802.1x Dashboard controls

Control	Description
Backend Authentication State	Displays the Backend Authentication State. The Backend Authentication state can be one of the following: • request • response • success • fail • timeout • idle
Reset	Re-initializes the 802.1x access-control parameters for the port. The following actions take place, depending on the 802.1x port configuration: • **force unauth:** the port is placed in unauthorized state, and traffic is blocked. • **auto:** the port is placed in unauthorized state, then authentication is initiated. • **force auth:** the port is placed in authorized state, and authentication is not required.
Reauthenticate	Re-authenticates the supplicant (client) attached to the port. This command only applies if the port's 802.1x mode is configured as `auto`.

VLANs Dashboard

To display the following form, select Layer 2 > **Virtual LANS** (click the underlined text, not the folder).



This form displays information for all configured VLANs and all member ports that have an active link state.

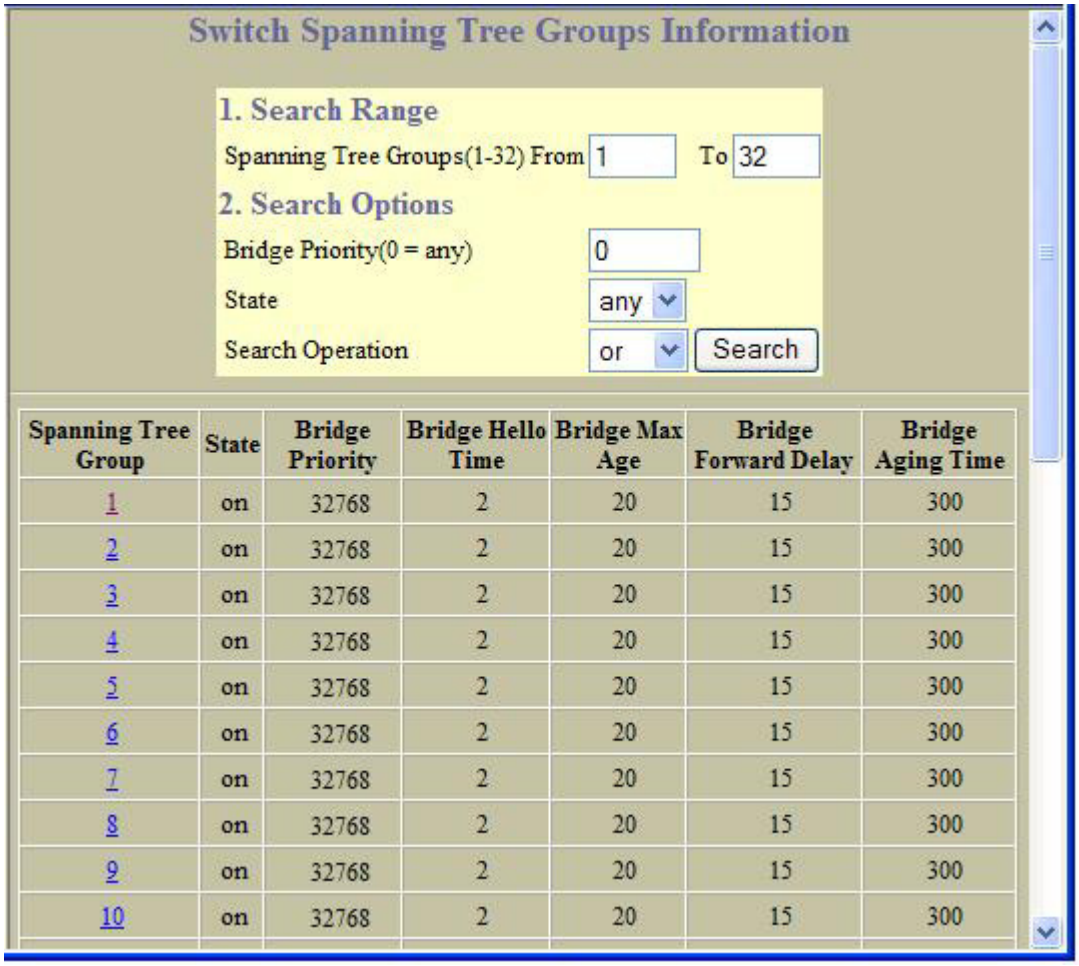
The following table describes the VLANs Dashboard controls:

Table 11 VLANs Dashboard controls

Control	Description
Search Range	To search for a VLAN, enter a range of VLAN numbers in the **From** and **To** fields.
Search Options	To focus the search for a VLAN, enter optional search parameters: • VLAN Name • VLAN State Fields that have a value of "any" are ignored during the search. Choose a search operation: • **or**: Search for VLANS specified in the search range that meet any of the criteria entered. • **and**: Search for VLANS specified in the search range that meet all of the criteria entered. Click **Search** to display VLANS that fit the range and meet the criteria entered.
VLAN ID	Displays the numeric identifier of the VLAN.
VLAN Name	Displays the name of the VLAN.
VLAN Ports	Displays the port numbers of ports that are members of the VLAN.
State	Shows if the VLAN is **enabled** or **disabled**.

Switch Spanning Tree Groups Information

To display the following form, select **Layer 2 > Spanning Tree Groups** (click the underlined text, not the folder).



Spanning Tree Group	State	Bridge Priority	Bridge Hello Time	Bridge Max Age	Bridge Forward Delay	Bridge Aging Time
1	on	32768	2	20	15	300
2	on	32768	2	20	15	300
3	on	32768	2	20	15	300
4	on	32768	2	20	15	300
5	on	32768	2	20	15	300
6	on	32768	2	20	15	300
7	on	32768	2	20	15	300
8	on	32768	2	20	15	300
9	on	32768	2	20	15	300
10	on	32768	2	20	15	300

The following table describes the Switch Spanning Tree Groups Information controls:

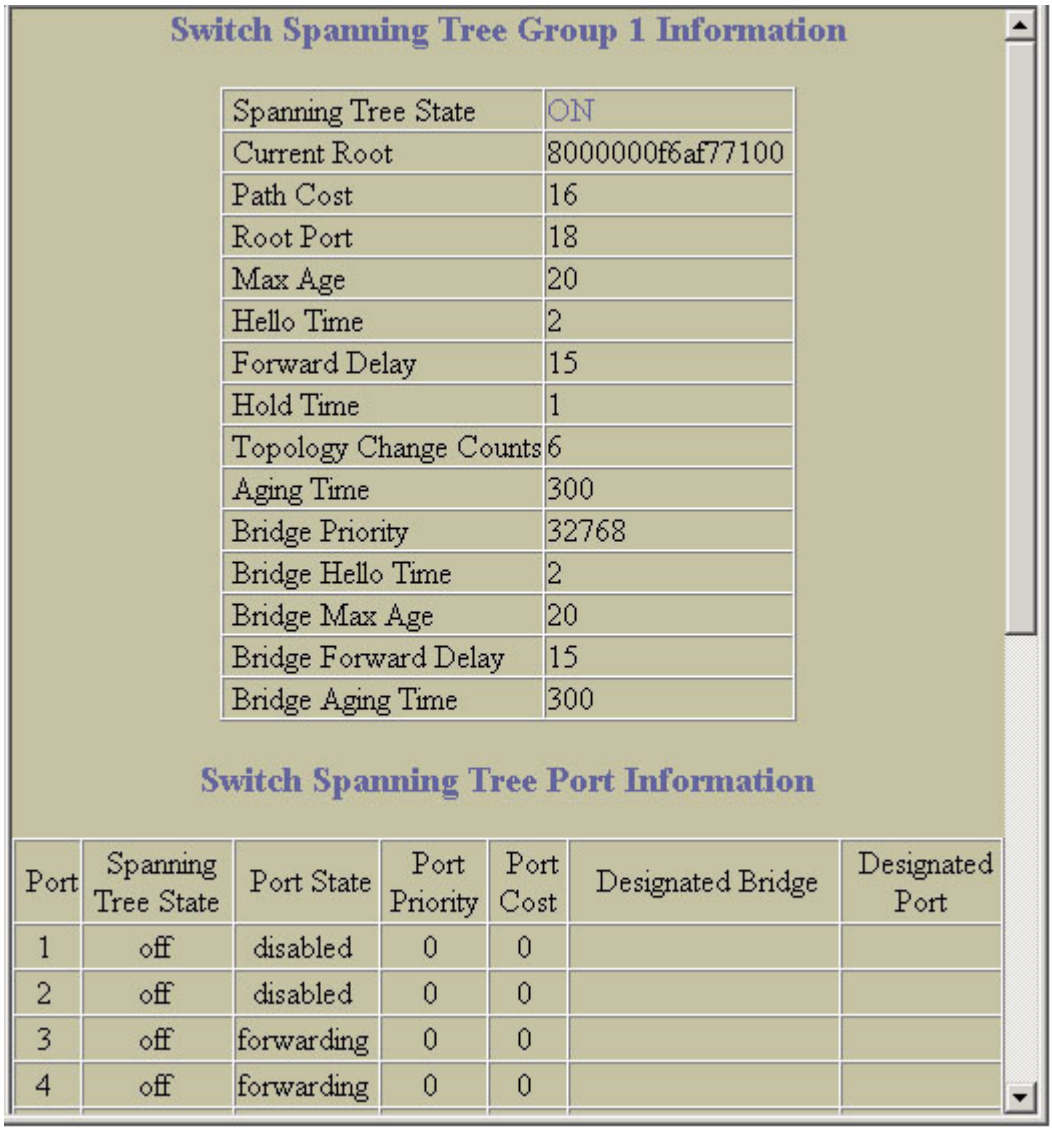
Table 12 Switch Spanning Tree Groups Information controls

Control	Description
Search Range	To search for a Spanning Tree Group, enter a range of group numbers in the **From** and **To** fields.
Search Options	To focus the search for a Spanning Tree Group, enter optional search parameters: • Bridge Priority • Spanning Tree State Fields that have a value of "any" are ignored during the search. Choose a search operation: • **or**: Search for spanning tree groups specified in the search range that meet any of the criteria entered. • **and**: Search for spanning tree groups specified in the search range that meet all of the criteria entered. Click **Search** to display spanning tree groups that fit the range and meet the criteria entered.
Spanning Tree Group	Displays the numeric identifier of the Spanning Tree Group.
State	Shows if Spanning Tree is turned **on** or **off** for the port.
Bridge Priority	Controls which bridge on the network will become the STP root bridge. This command does not apply to MSTP.
Bridge Hello Time	Specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value. This command does not apply to MSTP.
Bridge Max Age	Specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the STP network. This command does not apply to MSTP.
Bridge Forward Delay	Specifies, in seconds, the amount of time that a bridge port has to wait before it changes from learning state to forwarding state. This command does not apply to MSTP.
Bridge Aging Time	Specifies, in seconds, the amount of time the bridge waits without receiving a packet from a station before removing the station from the Forwarding Database.

Select a Spanning Tree Group number to display detailed information.

Switch Spanning Tree Group Information

To display the following form, go to the Switch Spanning Tree Groups Information form. Select a Spanning Tree Group number.



Switch Spanning Tree Group 1 Information

Spanning Tree State	ON
Current Root	8000000f6af77100
Path Cost	16
Root Port	18
Max Age	20
Hello Time	2
Forward Delay	15
Hold Time	1
Topology Change Counts	6
Aging Time	300
Bridge Priority	32768
Bridge Hello Time	2
Bridge Max Age	20
Bridge Forward Delay	15
Bridge Aging Time	300

Switch Spanning Tree Port Information

Port	Spanning Tree State	Port State	Port Priority	Port Cost	Designated Bridge	Designated Port
1	off	disabled	0	0		
2	off	disabled	0	0		
3	off	forwarding	0	0		
4	off	forwarding	0	0		

The following table describes the Switch Spanning Tree Group Information controls:

Table 13 Switch Spanning Tree Group Information controls

Control	Description
Spanning Tree State	Shows if Spanning Tree is turned **on** or **off** for the switch.
Current Root	Shows information about the root bridge for the Spanning Tree. Information includes the priority (hex) and MAC address of the root.
Path Cost	Displays the cumulative path cost to the Current Root.
Root Port	Displays the switch port that is connected to the Current Root.
Max Age	Specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the STP network.
Hello Time	Specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
Forward Delay	Specifies, in seconds, the amount of time that a bridge port has to wait before it changes from learning state to forwarding state.
Hold Time	Displays the minimum number of seconds that must elapse between transmissions of consecutive configuration BPDUs on a port.
Topology Change Counts	Displays the number of times the spanning tree topology has changed.
Aging Time	Specifies, in seconds, the amount of time the bridge waits without receiving a packet from a station before removing the station from the Forwarding Database.
Bridge Priority	Controls which bridge on the network will become the STP root bridge.
Bridge Hello Time	Specifies, in seconds, how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value.
Bridge Max Age	Specifies, in seconds, the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the STP network.
Bridge Forward Delay	Specifies, in seconds, the amount of time that a bridge port has to wait before it changes from learning state to forwarding state.
Bridge Aging Time	Specifies, in seconds, the amount of time the bridge waits without receiving a packet from a station before removing the station from the Forwarding Database.

Switch Spanning Tree Port Information

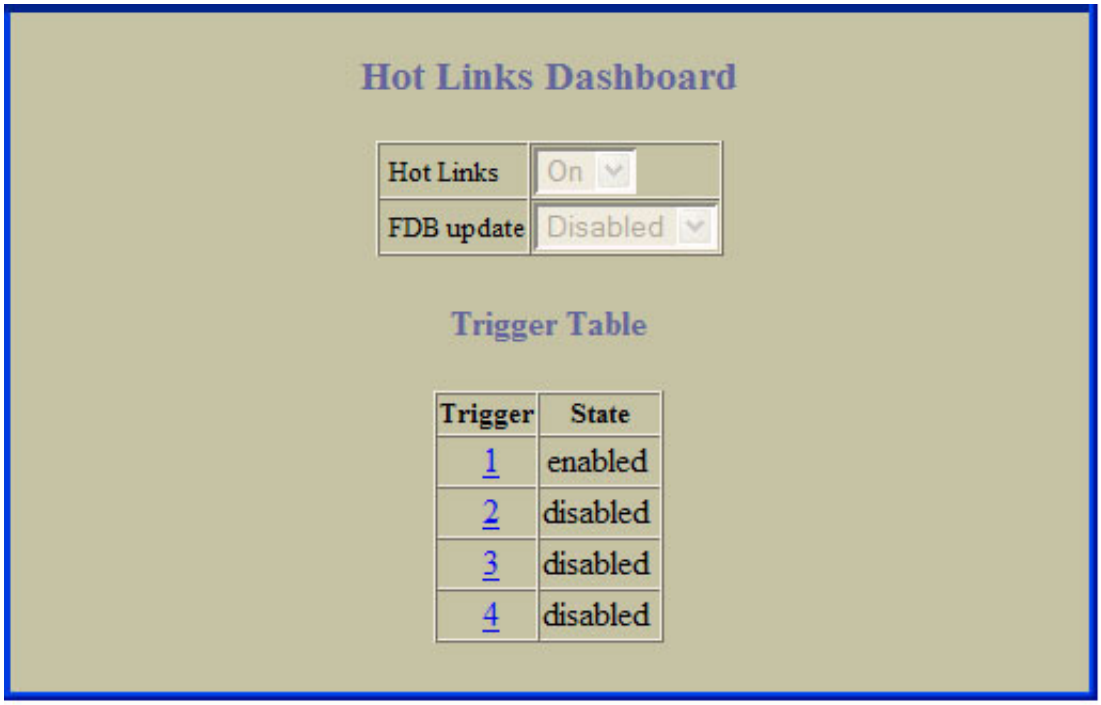
The following table describes the STP port parameters:

Table 14 Switch Spanning Tree Port Information controls

Control	Description
Port	Displays the port number for each port's STP information.
Spanning Tree State	Shows if Spanning Tree is turned **on** or **off** for the port.
Port State	Shows the current state of the port. The state field can be `blocking`, `listening`, `learning`, `forwarding`, or `disabled`. The State field in RSTP or MSTP mode can be one of the following: `Discarding (DISC), Learning (LRN), Forwarding (FWD), or Disabled (DSB).`
Port Priority	Helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment.
Port Cost	Helps determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. A setting of 0 indicates that the cost will be set to the appropriate default after the link speed has been auto negotiated.
Designated Bridge	Shows information about the bridge connected to each port, if applicable. Information includes the priority (hex) and MAC address of the Designated Bridge.
Designated Port	Displays the port ID of the port on the Designated Bridge to which this port is connected.

Hot Links Dashboard

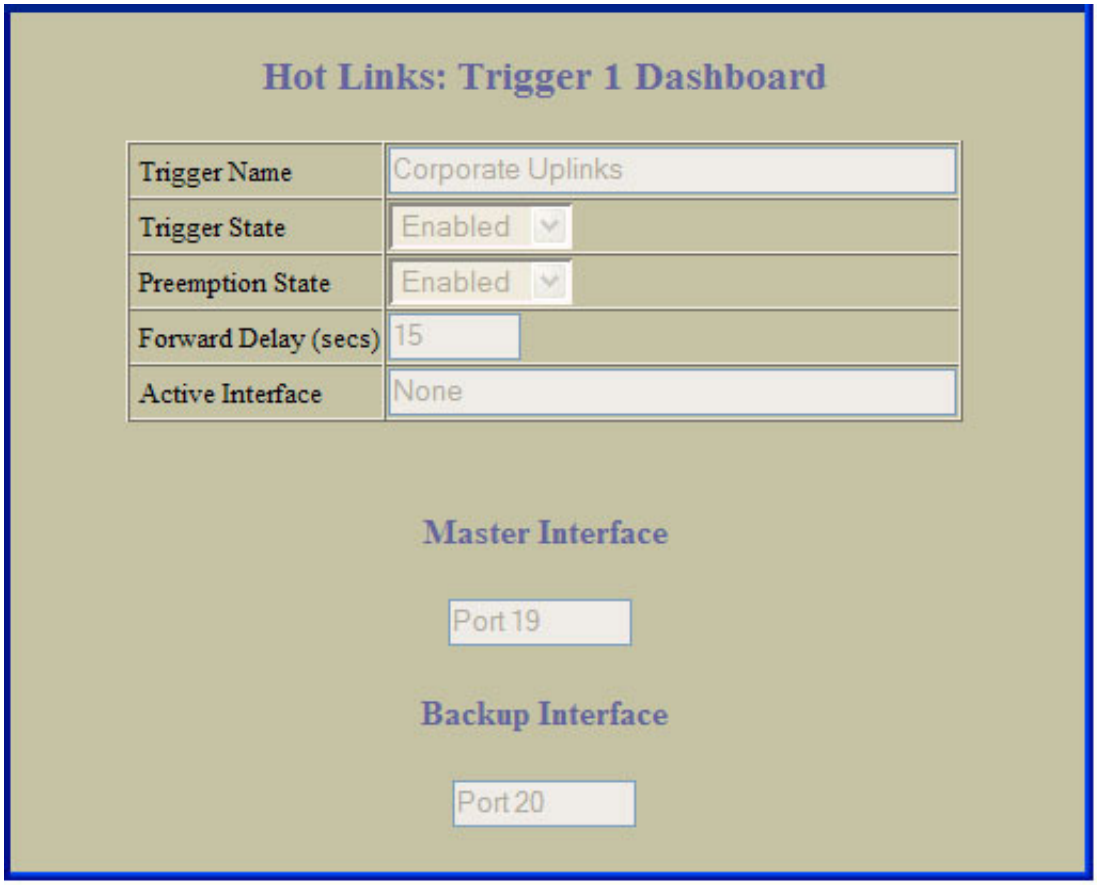
To display the following form, select **Layer 2 > Hot Links.**



This form summarizes Hot Links state information. Select a Hot Links Trigger number to display detailed information.

Hot Links Trigger Dashboard

To display the following form, go to the Hot Links Configuration form, and select a Trigger number.

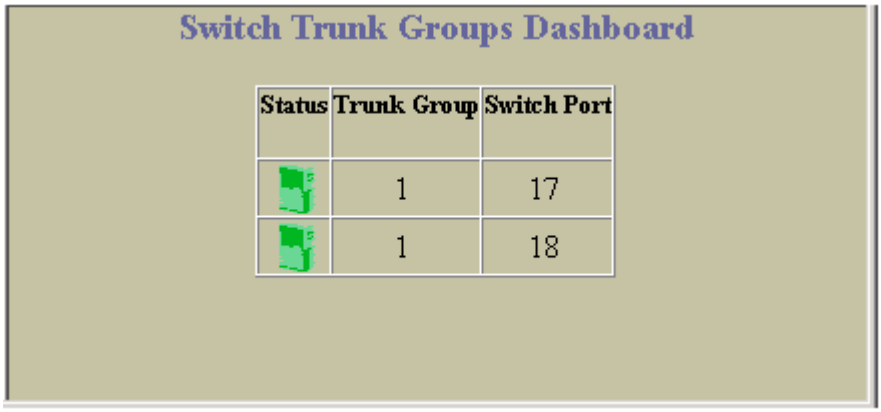


Hot Links Trigger information includes the following information:

- Trigger State (enabled or disabled)
- Pre-emption State (enabled or disabled)
- Forward Delay interval
- Active Interface (Master, Backup, or none)
- Master Interface port/trunk configuration
- Backup Interface port/trunk configuration

Switch Trunk Groups Dashboard

To display the following form, select **Layer 2 > Trunk Groups**.



When trunk groups are configured, you can view the state of each port in the various trunk groups.

NOTE: If Spanning Tree Protocol on any port in the trunk group is set to `forwarding`, the remaining ports in the trunk group will also be set to `forwarding`.

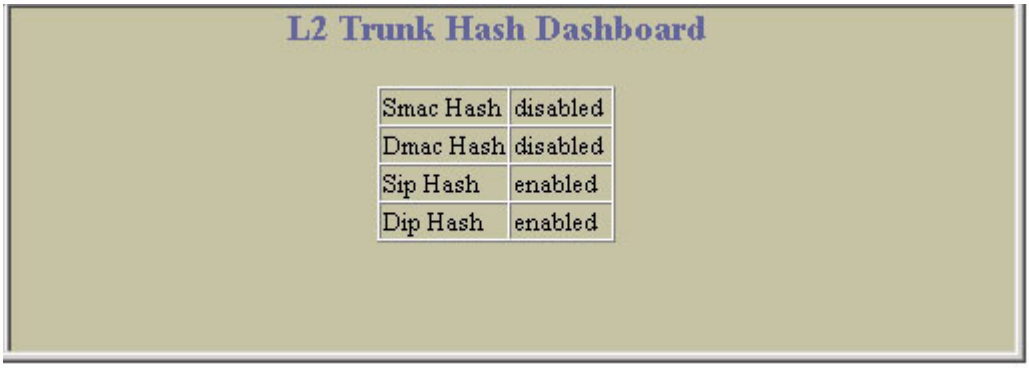
The following table describes the Switch Trunk Groups Dashboard controls:

Table 15 Switch Trunk Groups Dashboard controls

Control	Description
Status	Shows whether the Trunk Group is **enabled** (green) or **disabled** (red) on each port.
Trunk Group	Displays the numeric identifier of the Trunk Group.
Switch Port	Displays the port number of each port that is a member of the Trunk Group.

Trunk Hash Dashboard

To display the following form, select **Layer 2 > Trunk Hash**.



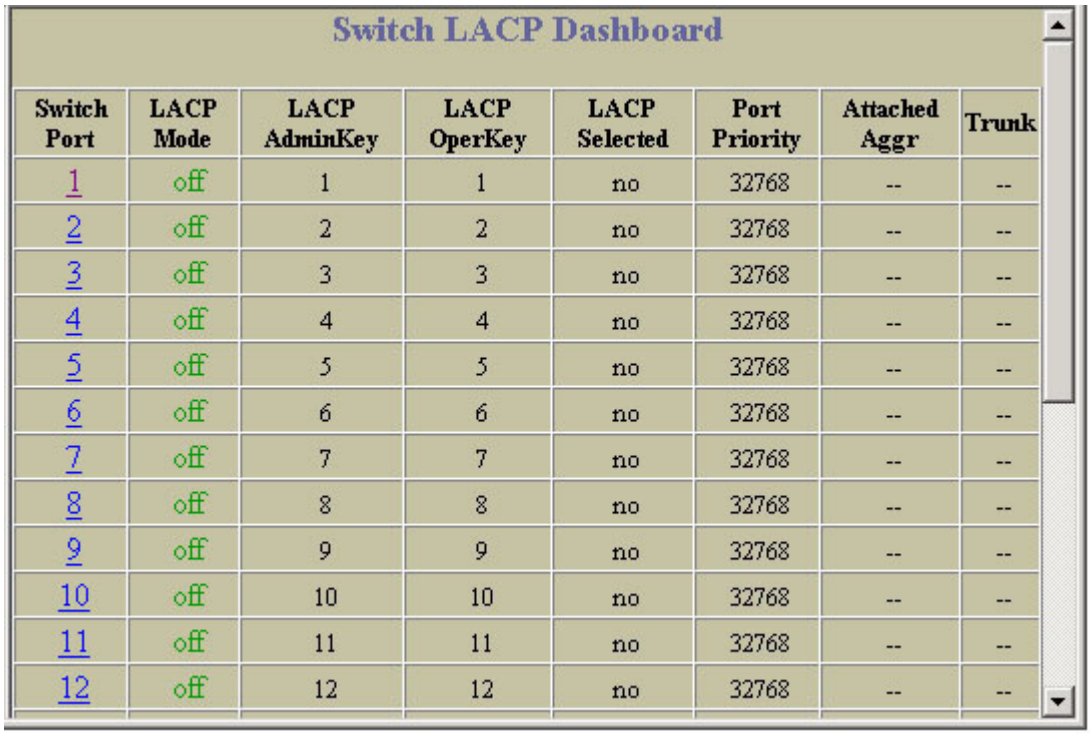
The following table describes the Layer 2 (L2) Trunk Hash Dashboard controls:

Table 16 Trunk Hash Dashboard controls

Control	Description
Smac Hash	Displays the status of the source MAC hash: **enabled** or **disabled**.
Dmac Hash	Displays the status of the destination MAC hash: **enabled** or **disabled**.
Sip Hash	Displays the status of the source IP hash: **enabled** or **disabled**.
Dip Hash	Displays the status of the source IP hash: **enabled** or **disabled**.

LACP Dashboard

To display the following form, select **Layer 2 > LACP**.



Switch LACP Dashboard

Switch Port	LACP Mode	LACP AdminKey	LACP OperKey	LACP Selected	Port Priority	Attached Aggr	Trunk
1	off	1	1	no	32768	--	--
2	off	2	2	no	32768	--	--
3	off	3	3	no	32768	--	--
4	off	4	4	no	32768	--	--
5	off	5	5	no	32768	--	--
6	off	6	6	no	32768	--	--
7	off	7	7	no	32768	--	--
8	off	8	8	no	32768	--	--
9	off	9	9	no	32768	--	--
10	off	10	10	no	32768	--	--
11	off	11	11	no	32768	--	--
12	off	12	12	no	32768	--	--

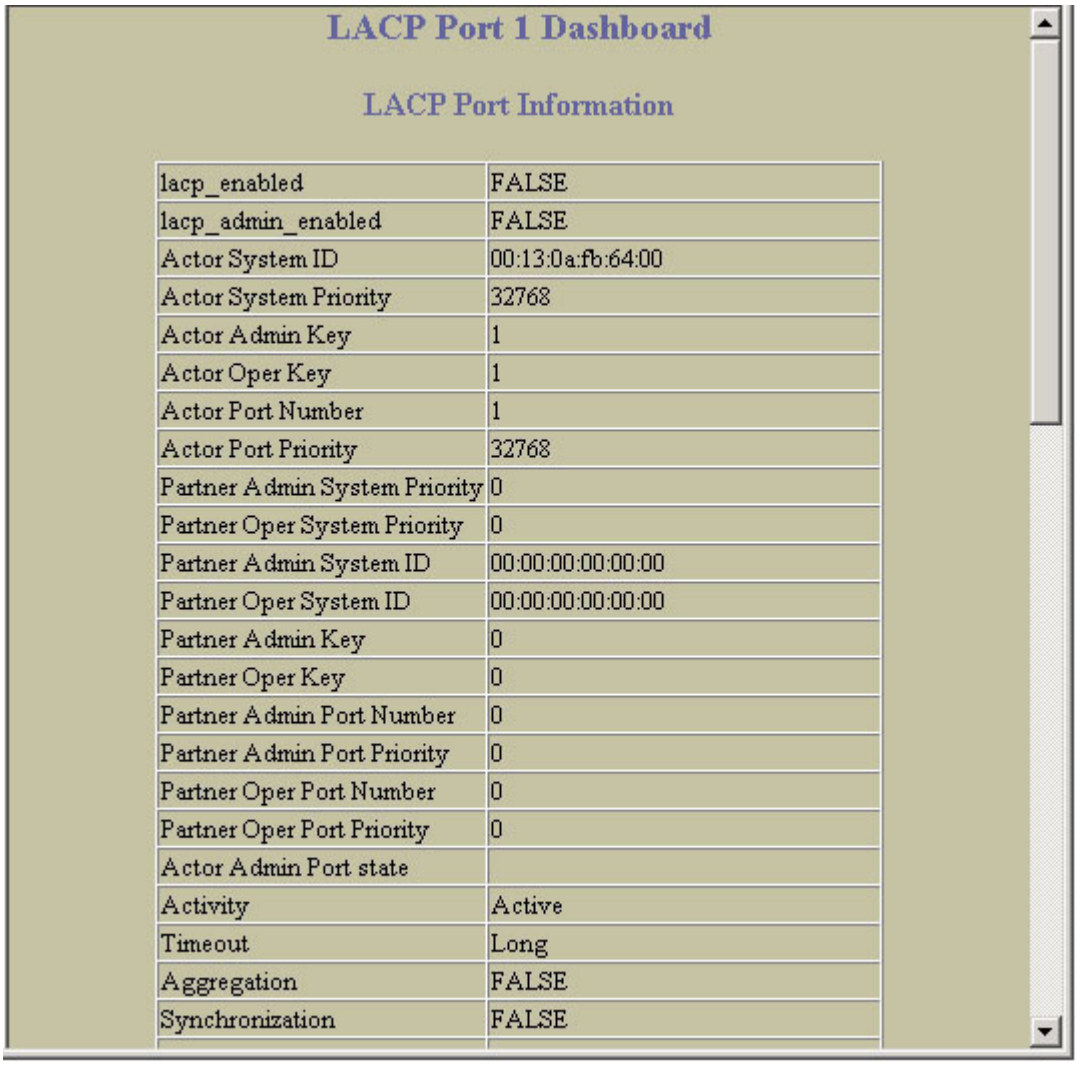
The following table describes the Switch LACP Dashboard controls:

Table 17 LACP Dashboard controls

Control	Description
Switch Port	Displays the port number.
LACP Mode	Displays the port's LACP mode (active, passive, or off).
LACP Adminkey	Displays the value of the port's *adminkey*.
LACP Operkey	Displays the value of the port's *operkey*.
LACP Selected	Indicates whether the port has been selected to be part of a Link Aggregation Group.
Port Priority	Shows the value of the port priority.
Attached Aggr	Displays the aggregator associated with each port.
Trunk	Displays the value that represents the LACP trunk group number.

LACP Port Dashboard

To display the following form, go to the Switch LACP Dashboard. Select a port number.



LACP Port 1 Dashboard

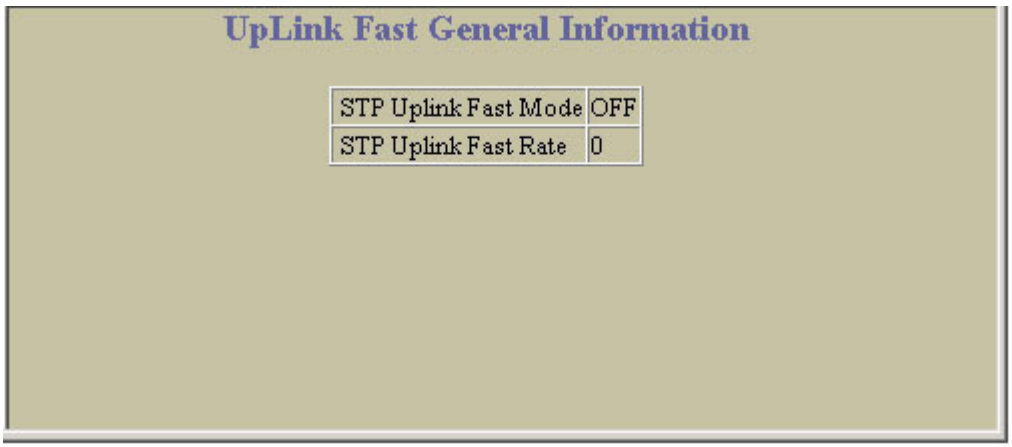
LACP Port Information

lacp_enabled	FALSE
lacp_admin_enabled	FALSE
Actor System ID	00:13:0a:fb:64:00
Actor System Priority	32768
Actor Admin Key	1
Actor Oper Key	1
Actor Port Number	1
Actor Port Priority	32768
Partner Admin System Priority	0
Partner Oper System Priority	0
Partner Admin System ID	00:00:00:00:00:00
Partner Oper System ID	00:00:00:00:00:00
Partner Admin Key	0
Partner Oper Key	0
Partner Admin Port Number	0
Partner Admin Port Priority	0
Partner Oper Port Number	0
Partner Oper Port Priority	0
Actor Admin Port state	
Activity	Active
Timeout	Long
Aggregation	FALSE
Synchronization	FALSE

This form summarizes LACP port information.

Uplink Fast General Information

To display the following form, select **Layer 2 > Uplink Fast**.



UpLink Fast General Information

STP Uplink Fast Mode	OFF
STP Uplink Fast Rate	0

The following table describes the Uplink Fast Information controls:

Table 18 Uplink Fast General Information controls

Control	Description
STP Uplink Fast Mode	Displays the status of STP Uplink Fast: ON or OFF.
STP Uplink Fast Rate	Displays the value of the Uplink Fast station update rate, in seconds.

Forwarding Database Information

To display the following form, select **Layer 2 > FDB**.

The forwarding database (FDB) contains information that maps the media access control (MAC) address of each known device to the switch port where the device address was learned. The FDB also shows which other ports have seen frames destined for a particular MAC address.

NOTE: The master forwarding database supports up to 8K MAC address entries on the MP per switch.

The following table describes the Forwarding Database Information controls:

Table 19 Forwarding Database Information controls

Control	Description
Show Entries of a Specific Source Port	Displays FDB entries for the selected port(s).
Show Entries of a Specific State	Displays FDB entries by state.
Show Entries of a Specific VLAN	Displays FDB entries for the selected VLAN.

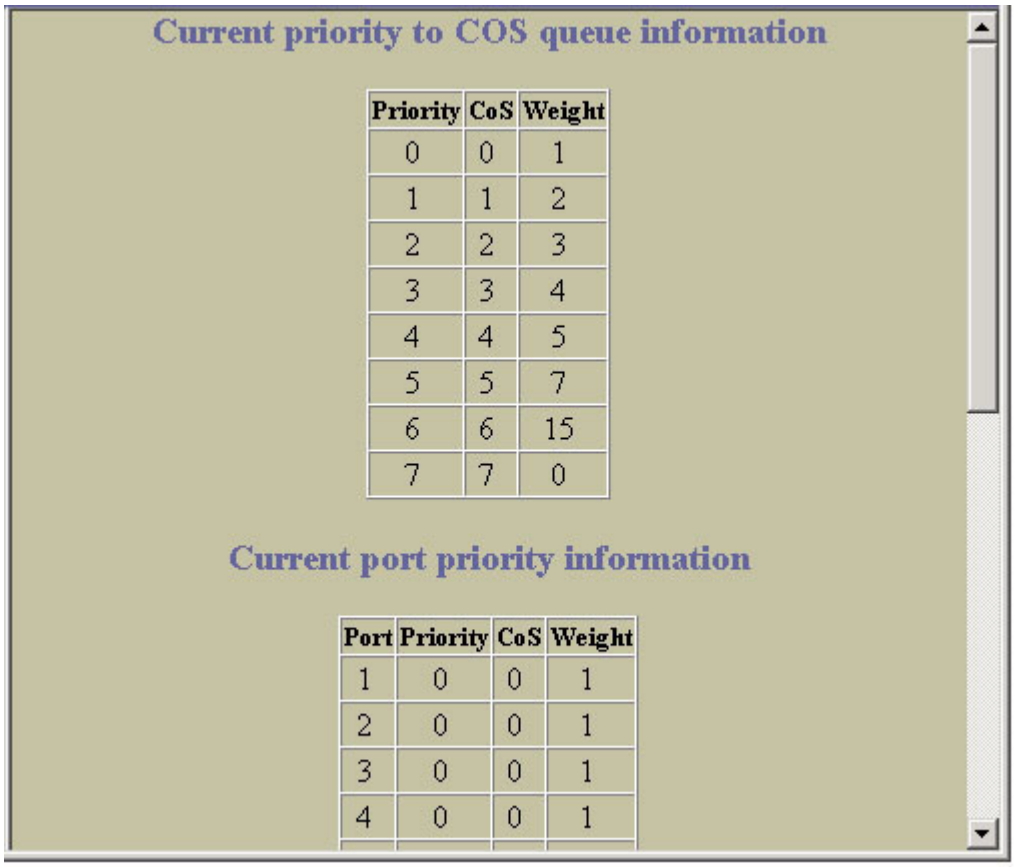
Table 19 Forwarding Database Information controls

Control	Description
Show Entry of a Specific MAC address	Displays a single FDB entry by IP address. Enter the MAC address using the format, `xx:xx:xx:xx:xx:xx`. For example, `08:00:20:12:34:56`
Clear FDB	Removes all FDB entries.
Entry #	Displays the numeric identifier of the FDB entry.
MAC Address	Displays the MAC address of the FDB entry.
VLAN	Displays the VLAN number of the FDB entry.
Source Port	Displays the source port of the FDB entry.
Trunk	Displays the trunk number of the FDB entry, if applicable.
State	Displays the port state of the FDB entry.
Learned Port	Displays the port number of the port that received the FDB entry.
Do you want to delete?	Click **Delete** to delete the FDB entry.
Permanent	Displays whether the FDB entry is a static, permanent entry.

An address that is in the forwarding (`FORWARD`) state means that the switch has learned it. When in the trunking (`TRUNK`) state, the port field represents the trunk group number. If the state for the port is listed as unknown (`UNKNOWN`), the MAC address has not yet been learned by the switch, but has only been seen as a destination address. When an address is in the unknown state, no outbound port is indicated.

802.1p Information

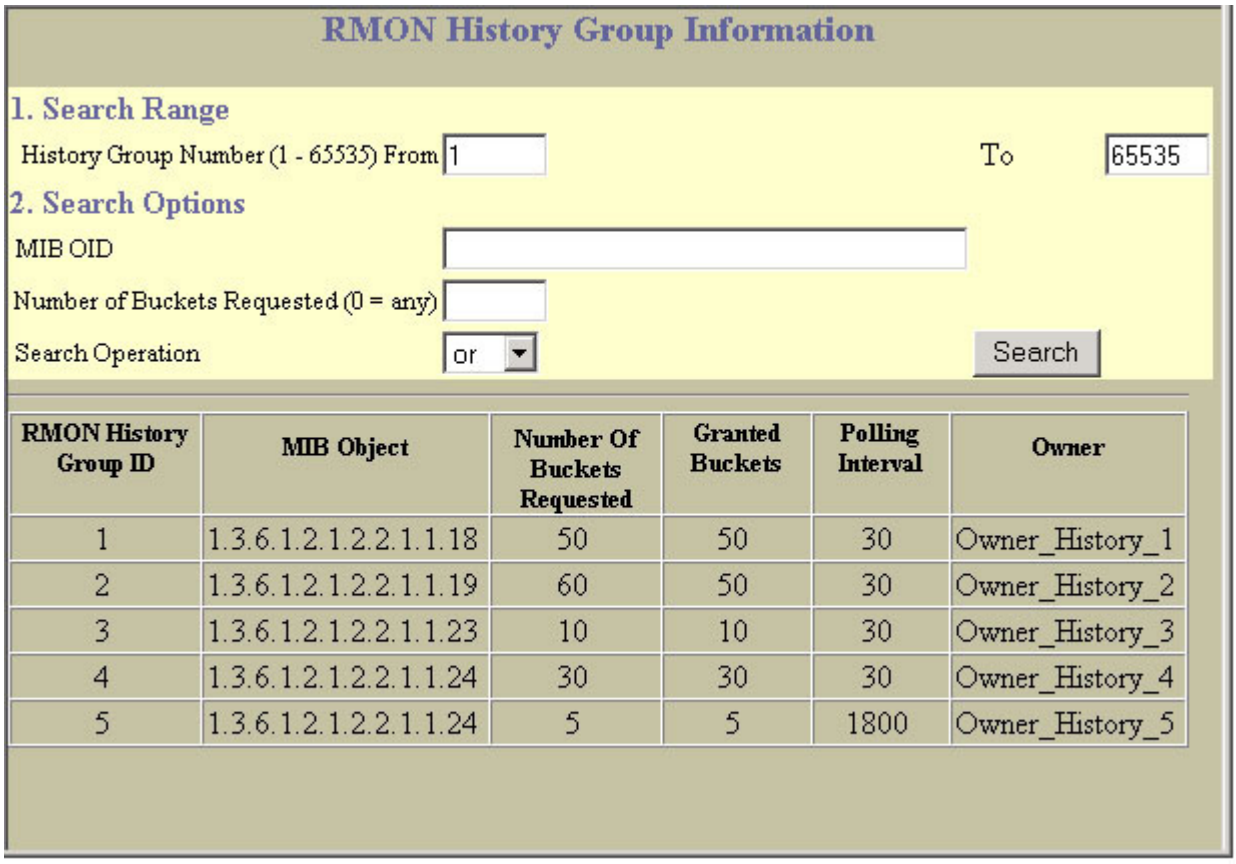
To display the following form, select **Layer 2 > 802.1p**.



This form shows the correlation between 802.1p priority values, Class of Service (COS) queues, and queue scheduling weights.

RMON History Group Information

To display the following form, select **RMON > History** (click the underlined text, not the folder).



This form displays information for all configured RMON History Groups.

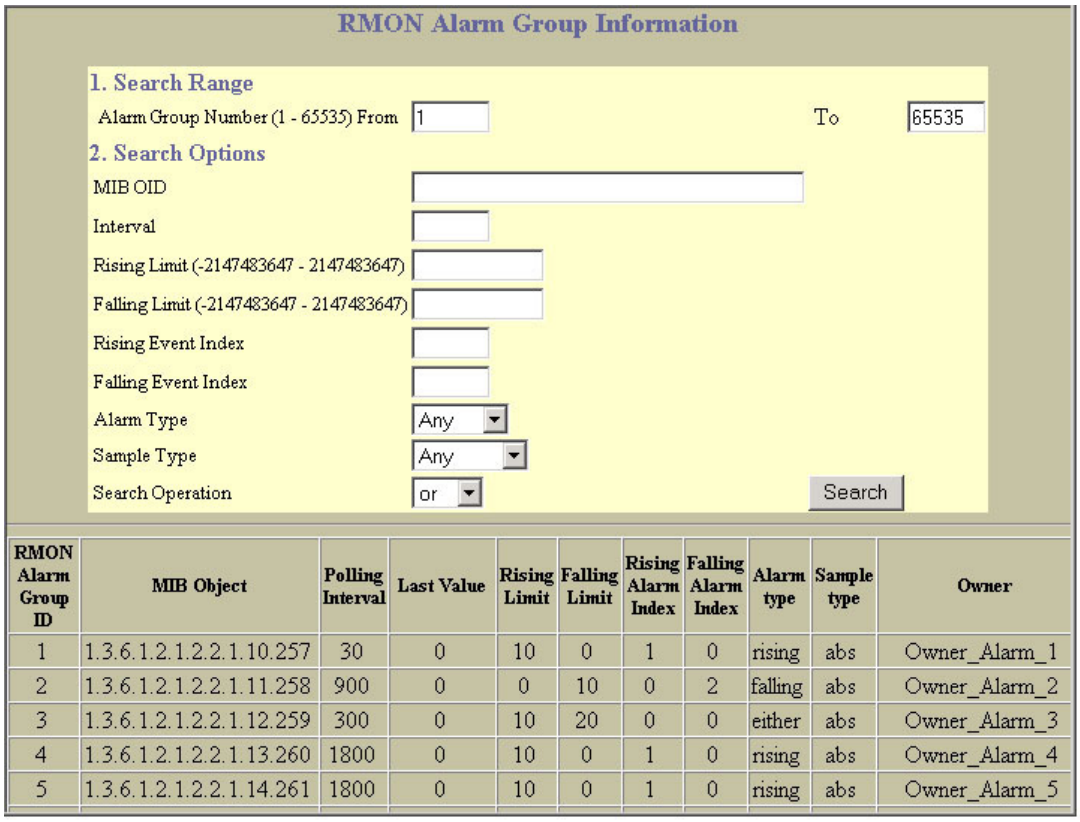
The following table describes the RMON History Group Dashboard controls:

Table 20 RMON History Group Dashboard controls

Control	Description
Search Range	To search for a History Group, enter a range of numbers in the **From** and **To** fields.
Search Options	To focus the search for a History Group, enter optional search parameters: • MIB OID • Number of buckets requested Fields that have a value of "any" are ignored during the search. Choose a search operation: • **or**: Search for History Groups specified in the search range that meet any of the criteria entered. • **and**: Search for History Groups specified in the search range that meet all of the criteria entered. Click **Search** to display History Groups that fit the range and meet the criteria entered.
RMON History Group ID	Displays the numeric identifier of the History Group.
MIB Object	Displays the MIB Object Identifier.
Number of Buckets Requested	Displays the number of requested buckets, which is the number of data slots into which data is to be saved.
Granted Buckets	Displays the number of granted buckets that may hold sampled data.
Polling Interval	Displays the time interval for each sampling bucket.
Owner	Displays a text string that identifies the person or entity that created this History Group.

RMON Alarm Group Information

To display the following form, select **RMON > Alarm** (click the underlined text, not the folder).



RMON Alarm Group ID	MIB Object	Polling Interval	Last Value	Rising Limit	Falling Limit	Rising Alarm Index	Falling Alarm Index	Alarm type	Sample type	Owner
1	1.3.6.1.2.1.2.2.1.10.257	30	0	10	0	1	0	rising	abs	Owner_Alarm_1
2	1.3.6.1.2.1.2.2.1.11.258	900	0	0	10	0	2	falling	abs	Owner_Alarm_2
3	1.3.6.1.2.1.2.2.1.12.259	300	0	10	20	0	0	either	abs	Owner_Alarm_3
4	1.3.6.1.2.1.2.2.1.13.260	1800	0	10	0	1	0	rising	abs	Owner_Alarm_4
5	1.3.6.1.2.1.2.2.1.14.261	1800	0	10	0	1	0	rising	abs	Owner_Alarm_5

This form displays information for all configured RMON Alarm Groups.

The following table describes the RMON Alarm Group Dashboard controls:

Table 21 RMON Alarm Group Dashboard controls

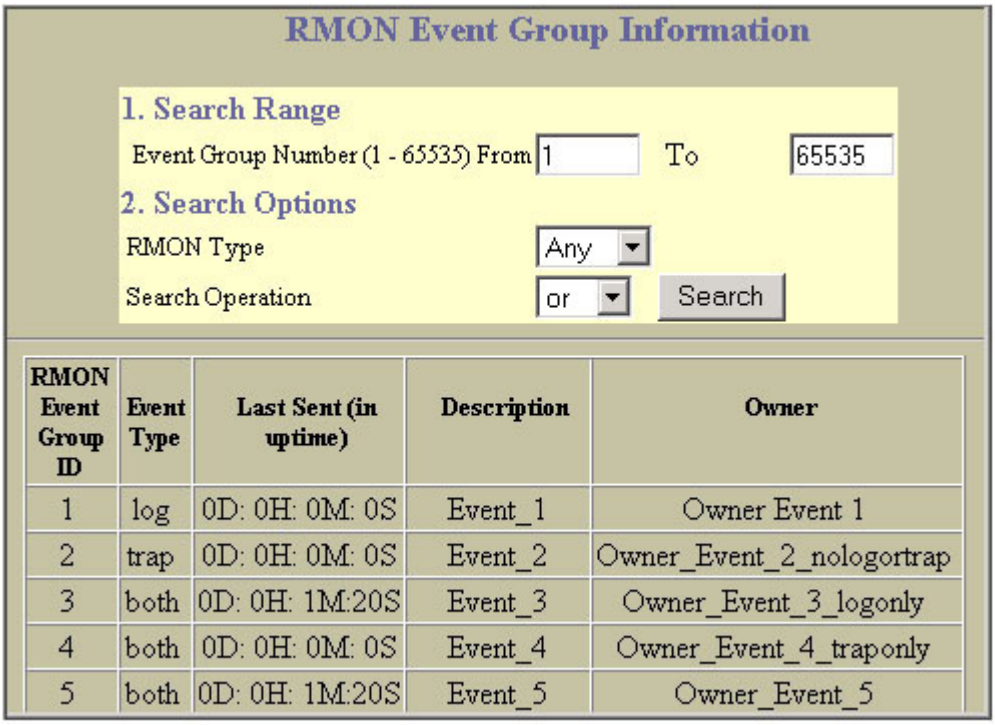
Control	Description
Search Range	To search for a RMON Alarm Group, enter a range of numbers in the **From** and **To** fields.
Search Options	To focus the search for a RMON Alarm, enter optional search parameters: • MIB OID • Interval • Rising Limit • Falling Limit • Rising Event Index • Falling Event Index • Alarm Type • Sample Type Fields that have a value of “any” are ignored during the search. Choose a search operation: • **or**: Search for Alarms specified in the search range that meet any of the criteria entered. • **and**: Search for Alarms specified in the search range that meet all of the criteria entered. Click **Search** to display RMON Alarms that fit the range and meet the criteria entered.
RMON Alarm Group ID	Displays the numeric identifier of the Alarm Group.
MIB Object	Displays the MIB Object Identifier.
Polling Interval	Displays the time interval over which data is sampled and compared with the rising and falling thresholds.
Last Value	Displays the most recent value sampled.
Rising Limit	Displays the rising threshold for the sampled statistic.
Falling Limit	Displays the falling threshold for the sampled statistic.

Table 21 RMON Alarm Group Dashboard controls

Control	Description
Rising Alarm Index	Displays the rising alarm event index that is triggered when a rising threshold is crossed.
Falling Alarm Index	Displays the falling alarm event index that is triggered when a falling threshold is crossed.
Alarm Type	Displays the alarm type as rising, falling, or either (rising or falling).
Sample Type	Displays the method of sampling the selected variable and calculating the value to be compared against the thresholds, as follows: • **abs**: absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. • **delta**: delta value, the value of the selected variable at the last sample is subtracted from the current value, and the difference compared with the thresholds.
Owner	Displays a text string that identifies the person or entity that created this Alarm Group.

RMON Event Group Information

To display the following form, select **RMON > Event** (click the underlined text, not the folder).



This form displays information for all configured RMON Event Groups.

The following table describes the RMON Event Group Dashboard controls:

Table 22 RMON Event Group Dashboard controls

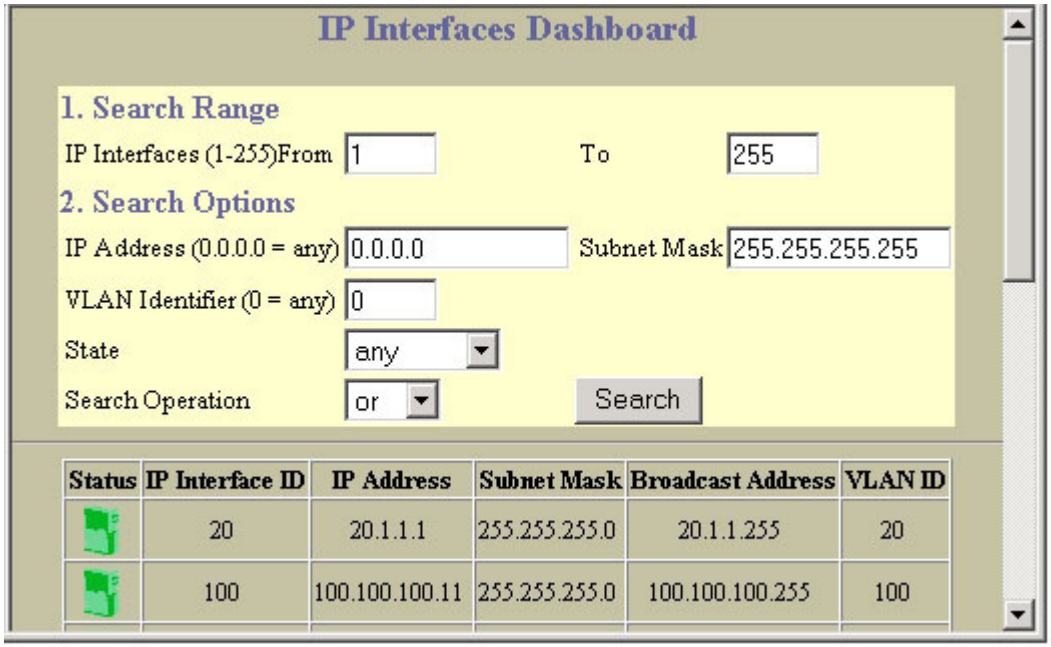
Control	Description
Search Range	To search for a RMON Event Group, enter a range of numbers in the **`From`** and **`To`** fields.
Search Options	To focus the search for an Event Group, enter the optional search parameter: RMON Type Fields that have a value of “any” are ignored during the search. Choose a search operation: **or**: Search for Events specified in the search range that meet any of the criteria entered. **and**: Search for Events specified in the search range that meet all of the criteria entered. Click **Search** to display Events that fit the range and meet the criteria entered.
RMON Event Group ID	Displays the numeric identifier of the Event Group.

Table 22 RMON Event Group Dashboard controls

Control	Description
Event Type	Displays the type of notification provided for this event, as follows: `none, log, trap, both`.
Last Sent	Displays the time that passed since the last switch reboot, when the most recent event was triggered. This value is cleared when the switch reboots.
Description	Displays a text description of the event.
Owner	Displays a text string that identifies the person or entity that created this Event Group.

IP Interfaces Dashboard

To display the following form, select **Layer 3 > IP Interfaces** (click the underlined text, not the folder).



The following table describes the IP Interfaces Dashboard controls:

Table 23 IP Interfaces Dashboard controls

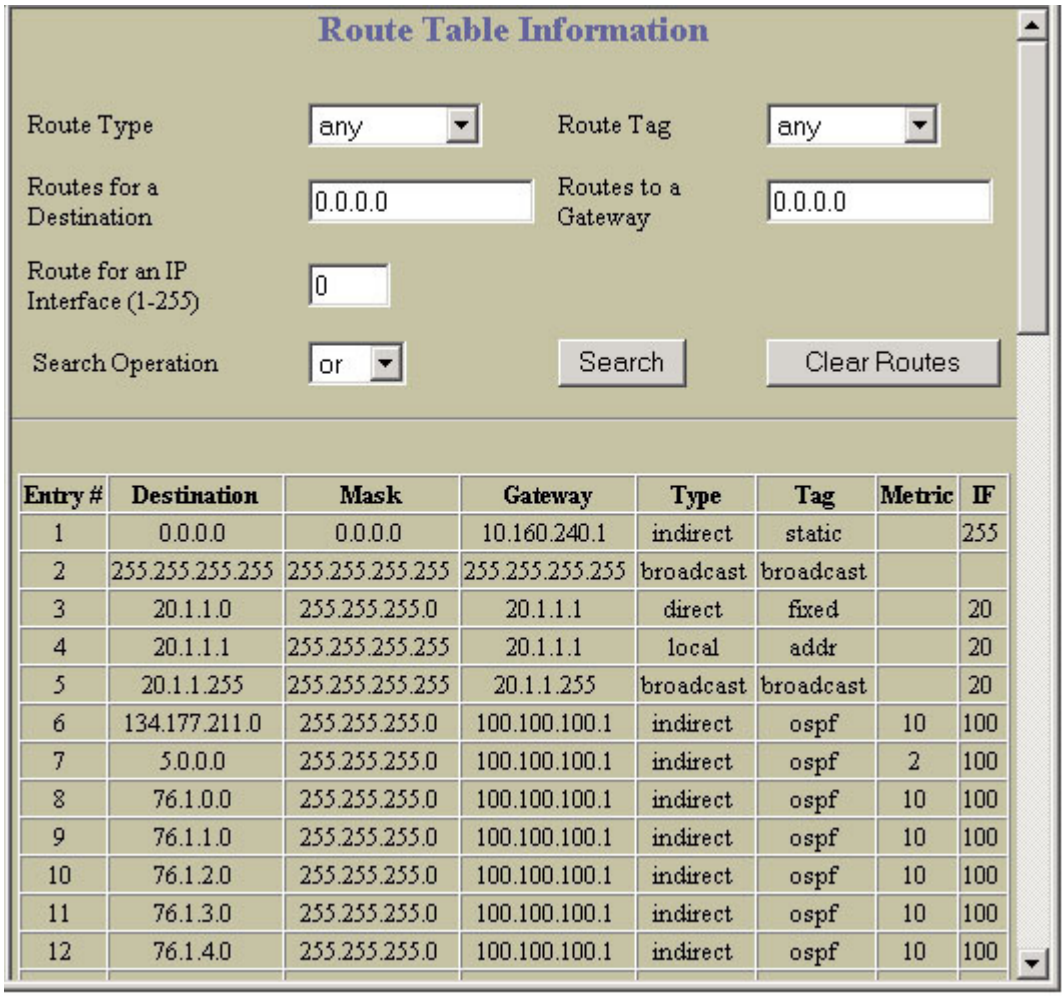
Control	Description
Search Range	To search for an IP Interface, enter a range of IP Interface numbers in the **From** and **To** fields.
Search Options	To focus the search for an IP Interface, enter optional search parameters: • IP Address • Subnet Mask • VLAN ID number • IP Interface State Fields that have a value of "any" are ignored during the search. Choose a search operation: • **or**: Search for IP Interfaces specified in the search range that meet any of the criteria entered. • **and**: Search for IP Interfaces specified in the search range that meet all of the criteria entered. Click **Search** to display IP Interfaces that fit the range and meet the criteria entered.
Status	Shows if the IP Interface is **enabled** (green) or **disabled** (red).
IP Interface ID	Displays the numeric identifier of the IP Interface.
IP Address	Displays the IP address of the IP Interface.
Subnet Mask	Displays the Subnet Mask of the IP Interface.

Table 23 IP Interfaces Dashboard controls

Control	Description
Broadcast Address	Displays the IP Broadcast address for this IP Interface.
VLAN ID	Displays the VLAN number for this interface. Each interface can belong to one VLAN, although any VLAN can have multiple IP interfaces in it.

Route Table Information

To display the following form, select **Layer 3 > Network Routes** (click the underlined text, not the folder).



Entry #	Destination	Mask	Gateway	Type	Tag	Metric	IF
1	0.0.0.0	0.0.0.0	10.160.240.1	indirect	static		255
2	255.255.255.255	255.255.255.255	255.255.255.255	broadcast	broadcast		
3	20.1.1.0	255.255.255.0	20.1.1.1	direct	fixed		20
4	20.1.1.1	255.255.255.255	20.1.1.1	local	addr		20
5	20.1.1.255	255.255.255.255	20.1.1.255	broadcast	broadcast		20
6	134.177.211.0	255.255.255.0	100.100.100.1	indirect	ospf	10	100
7	5.0.0.0	255.255.255.0	100.100.100.1	indirect	ospf	2	100
8	76.1.0.0	255.255.255.0	100.100.100.1	indirect	ospf	10	100
9	76.1.1.0	255.255.255.0	100.100.100.1	indirect	ospf	10	100
10	76.1.2.0	255.255.255.0	100.100.100.1	indirect	ospf	10	100
11	76.1.3.0	255.255.255.0	100.100.100.1	indirect	ospf	10	100
12	76.1.4.0	255.255.255.0	100.100.100.1	indirect	ospf	10	100

The following table describes the Route Table Information controls:

Table 24 Route Table Information controls

Control	Description
Search Operation	To focus the search for an IP static route, enter search parameters: • Route Type • Route Tag • Routes for a Destination IP • Routes to a Gateway IP • Route for an IP Interface Fields that have a value of "any" are ignored during the search. Choose a search operation: • **or**: Search for network routes specified in the Search range that meet any of the criteria entered. • **and**: Search for network routes specified in the Search range that meet all of the criteria entered. Click **Search** to display network routes that fit the range and meet the criteria entered.
Entry #	Displays the entry number for each route.

Table 24 Route Table Information controls

Control	Description
Destination	Displays the destination IP address fore the IP route.
Mask	Displays the subnet mask for the IP route.
Gateway	Displays the IP address of the gateway associated with the IP route.
Type	Displays the IP route type. See the IP Routing Type information table for more detail.
Tag	Displays the IP route tag. See the IP Routing Tag information table for more detail.
Metric	Displays the value of the IP route metric.
IF	Displays the interface number associated with the IP route.

The following table describes the Route Table `Type` parameter.

Table 25 IP Routing Type information

Field	Description
`indirect`	The next hop to the host or subnet destination will be forwarded through a router at the Gateway address.
`direct`	Packets will be delivered to a destination host or subnet attached to the switch.
`local`	Indicates a route to one of the switch's IP interfaces.
`broadcast`	Indicates a broadcast route.
`martian`	The destination belongs to a host or subnet which is filtered out. Packets to this destination are discarded.
`multicast`	Indicates a multicast route.

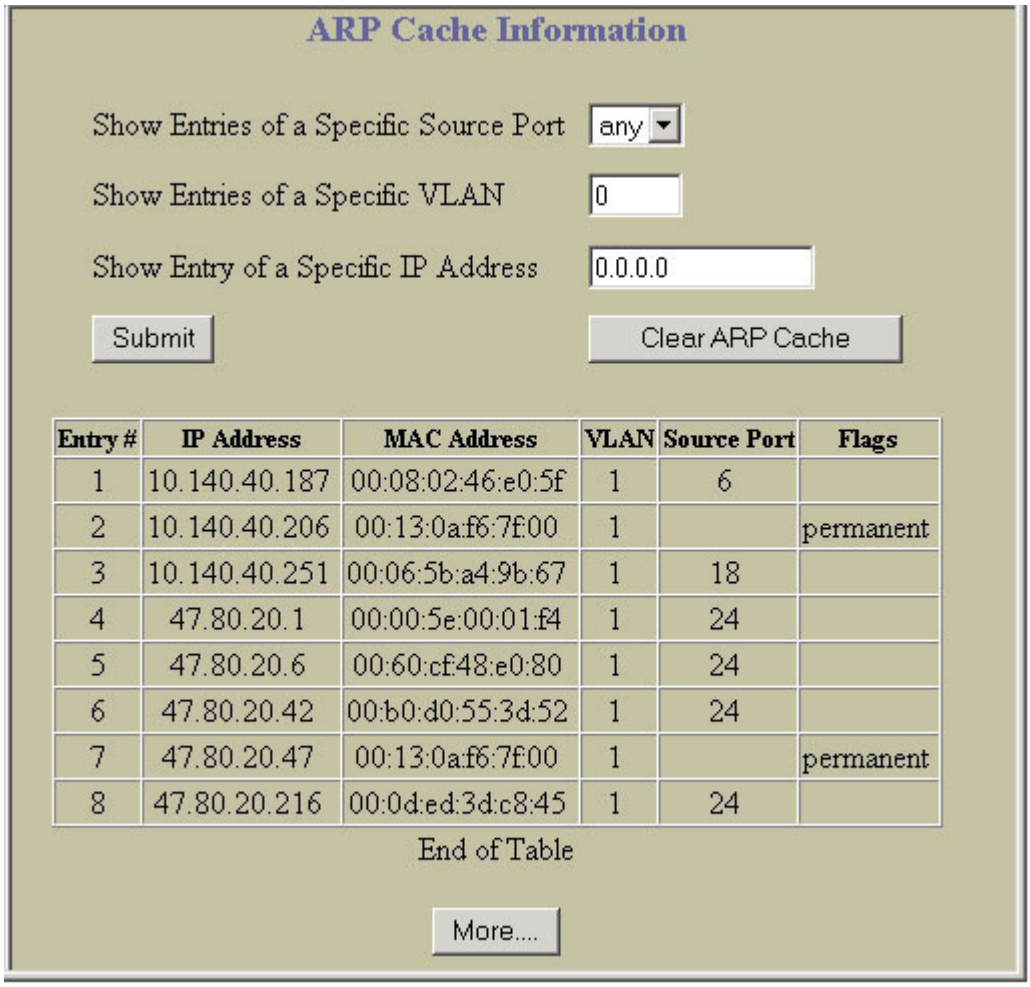
The following table describes the Route Table `Tag` parameter.

Table 26 IP Routing Tag information

Field	Description
`fixed`	The address belongs to a host or subnet attached to the switch.
`static`	The address is a static route which has been configured on the GbE2 Switch.
`addr`	The address belongs to one of the switch's IP interfaces.
`rip`	The address was learned by the Routing Information Protocol (RIP).
`ospf`	The address was learned by Open Shortest Path First (OSPF).
`broadcast`	The address is a broadcast address.
`multicast`	The address is a multicast address.
`martian`	The address belongs to a filtered group.

ARP Cache Information

To display the following form, select **Layer 3 > ARP** (click the underlined text, not the folder).



The ARP information includes IP address and MAC address of each entry, address status flags, VLAN, and port for the address, and port referencing information.

The following table describes the ARP Cache Information controls:

Table 27 ARP Cache Information controls

Control	Description
Show Entries of a Specific Source Port	Displays ARP entries for the selected port(s).
Show Entries of a Specific VLAN	Displays ARP entries for the selected VLAN.
Show Entry of a Specific IP Address	Displays a single ARP entry by IP address.
Clear ARP Cache	Clears the ARP data cache.
Entry #	Displays the numeric identifier of the ARP entry.
IP Address	Displays the IP address of the ARP entry.
MAC Address	Displays the MAC address of the ARP entry.
VLAN	Displays the VLAN number of the port where the ARP entry request is received.
Source Port	Displays the source port of the ARP entry.
Flags	Displays the address status flag for the ARP entry.

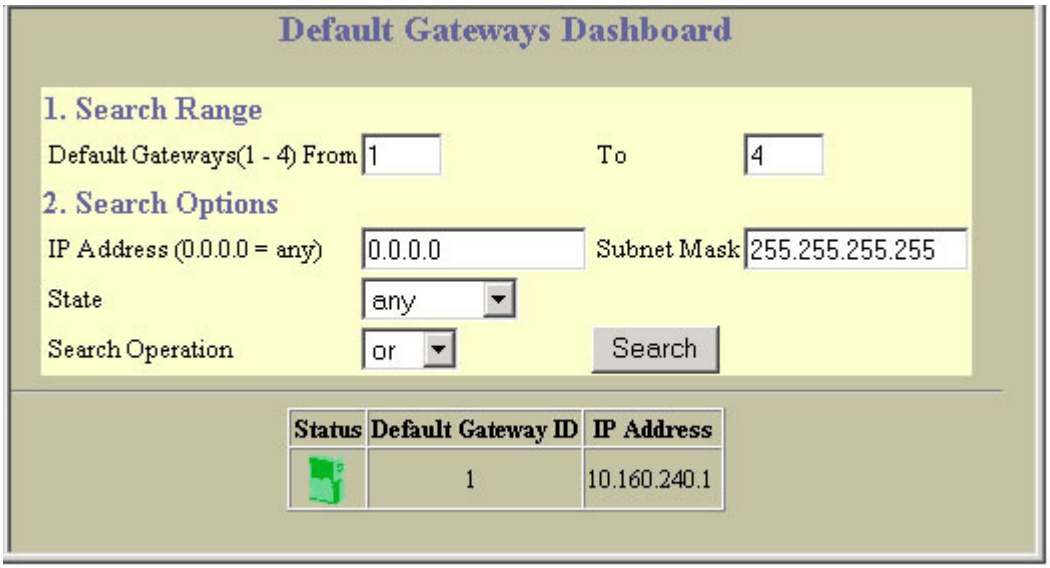
The **Flags** field is interpreted as follows:

Table 28 ARP Dump Flag Parameters

Flag	Description
Interface	Permanent entry created for switch IP interface
Indirect	Indirect route entry
Unresolved	Unresolved ARP entry. The MAC address has not been learned.

Default Gateways Dashboard

To display the following form, select **Layer 3 > Default Gateways** (click the underlined text, not the folder).



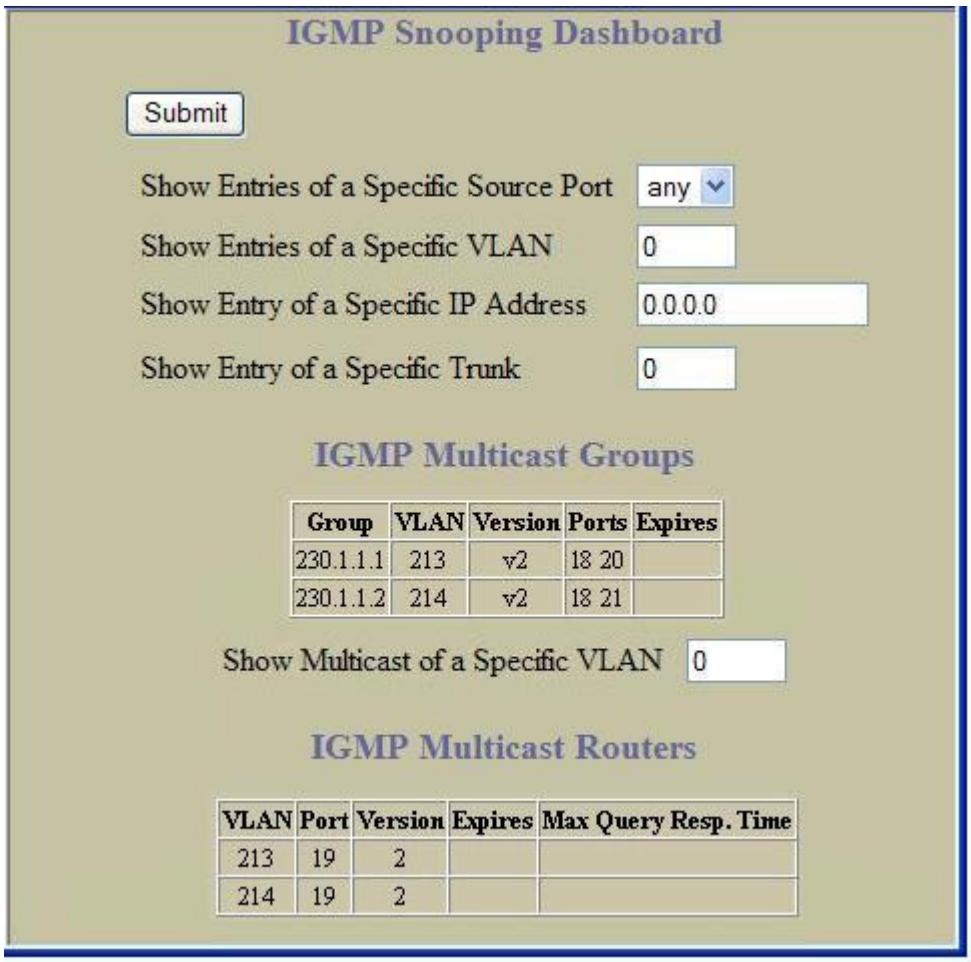
The following table describes the Default Gateways Dashboard controls:

Table 29 Default Gateways Dashboard controls

Control	Description
Search Range	To search for a Default Gateway, enter a range of Gateway numbers in the **From** and **To** fields.
Search Options	To focus the search for a Default Gateway, enter optional search parameters: • IP Address • Subnet Mask • Default Gateway State Fields that have a value of "any" are ignored during the search. Choose a search operation: **or**: Search for Default Gateways specified in the search range that meet any of the criteria entered. **and**: Search for Default Gateways specified in the search range that meet all of the criteria entered. Click **Search** to display Default Gateways that fit the range and meet the criteria entered.
Status	Shows if the Default Gateway is **enabled** (green) or **disabled** (red).
Default Gateway ID	Displays the numeric identifier of the Default Gateway.
IP Address	Displays the IP Address of the Default Gateway.

IGMP Snooping Dashboard

To display the following form, select **Layer 3 > IGMP > IGMP Snooping** (click the underlined text, not the folder).



IGMP Multicast Groups

The following table describes the IGMP Multicast Groups information.

Table 30 IGMP Multicast Groups information

Field	Description
Group	Displays the IP address of the IGMP Multicast Group.
VLAN	Displays the VLAN number of the IGMP Multicast Group.
Version	Displays the IGMP version.
Ports	Displays the port numbers of ports that carry IGMP Multicast traffic for the group.
Expires	Displays the time remaining until a Mrouter port is deleted from the Multicast IGMP table.

IGMP Multicast Routers

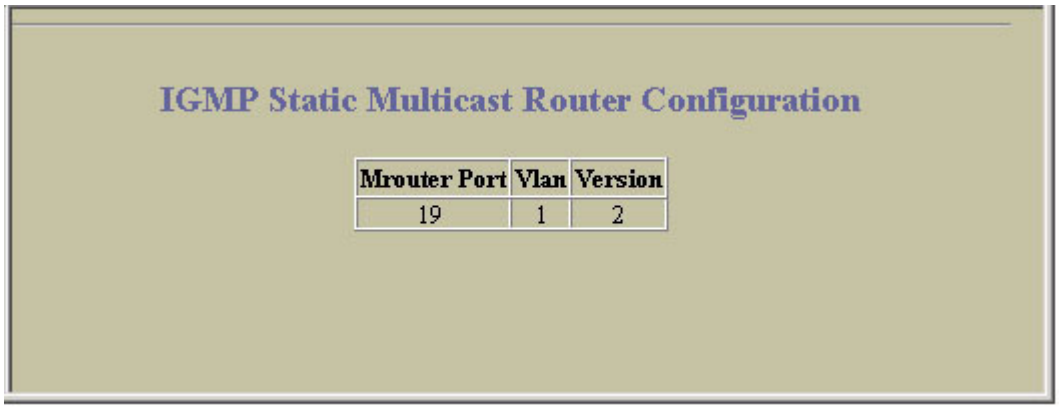
The following table describes the commands used to display information about IGMP Multicast Routers.

Table 31 IGMP Multicast Routers information

Field	Description
VLAN	Displays the VLAN number on which the Multicast Router resides.
Port	Displays the port to which the Multicast Router is connected.
Version	Displays the IGMP version.
Expires	Displays the time remaining until a Mrouter port is deleted from the Multicast IGMP table.
Max Query Resp. Time	Displays the maximum time allowed before responding to an IGMP Membership Query.

IGMP Static Multicast Router Configuration

To display the following form, select **Layer 3 > IGMP > IGMP Static Mrouter** (click the underlined text, not the folder).



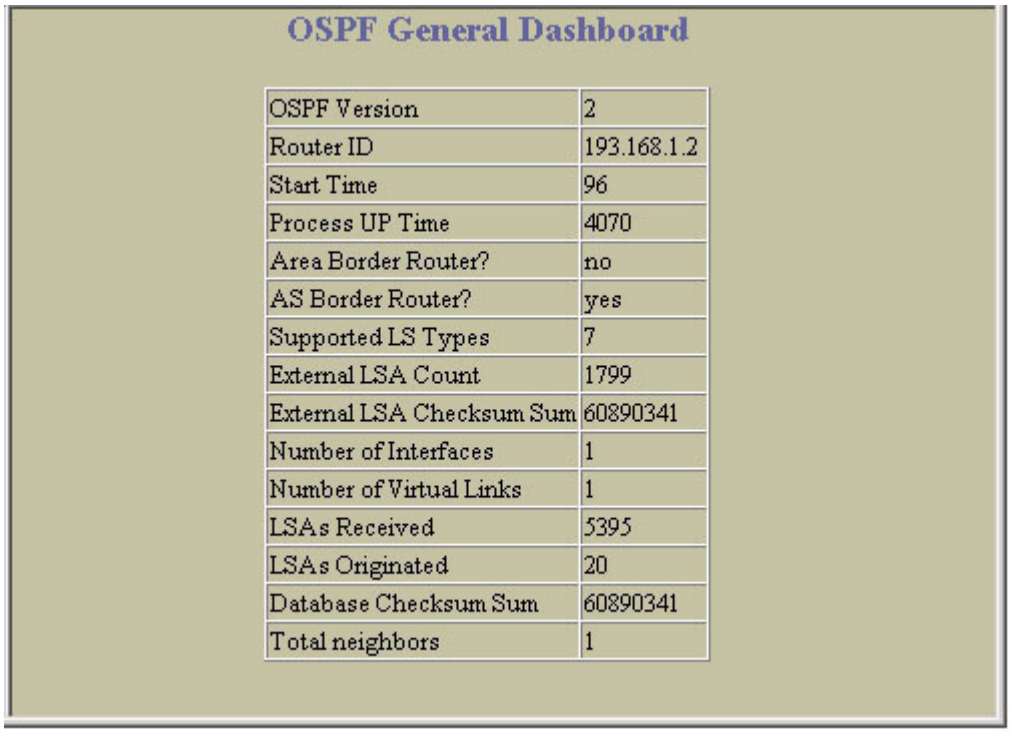
The following table describes the IGMP Static multicast router (Mrouter) information.

Table 32 IGMP Static Multicast Router information

Field	Description
Mrouter Port	Displays the port where the static Mrouter is configured.
VLAN	Displays the VLAN number of the IGMP Multicast Group.
Version	Displays the IGMP version.

OSPF General Dashboard

To display the following form, select **Layer 3 > OSPF > General.**



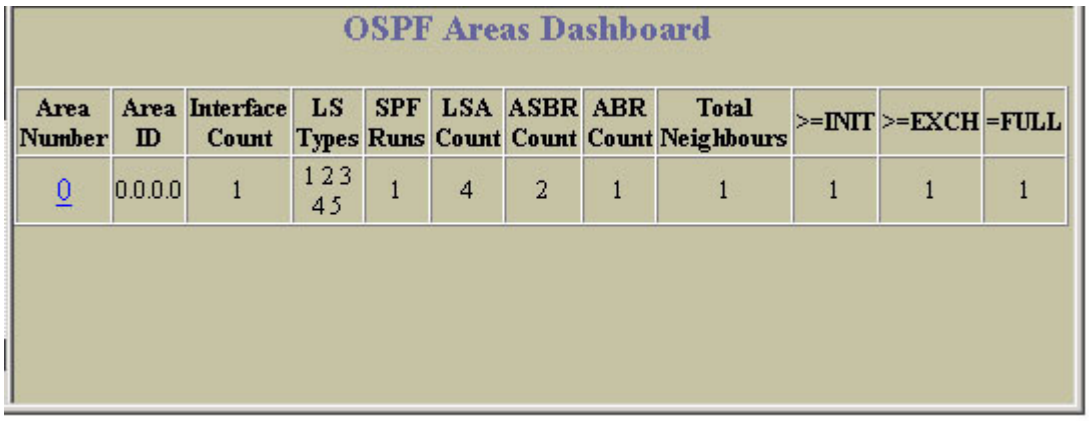
OSPF General Dashboard

OSPF Version	2
Router ID	193.168.1.2
Start Time	96
Process UP Time	4070
Area Border Router?	no
AS Border Router?	yes
Supported LS Types	7
External LSA Count	1799
External LSA Checksum Sum	60890341
Number of Interfaces	1
Number of Virtual Links	1
LSAs Received	5395
LSAs Originated	20
Database Checksum Sum	60890341
Total neighbors	1

This form summarizes general OSPF information.

OSPF Areas Dashboard

To display the following form, select **Layer 3 > OSPF > OSPF Areas** (click the underlined text, not the folder).



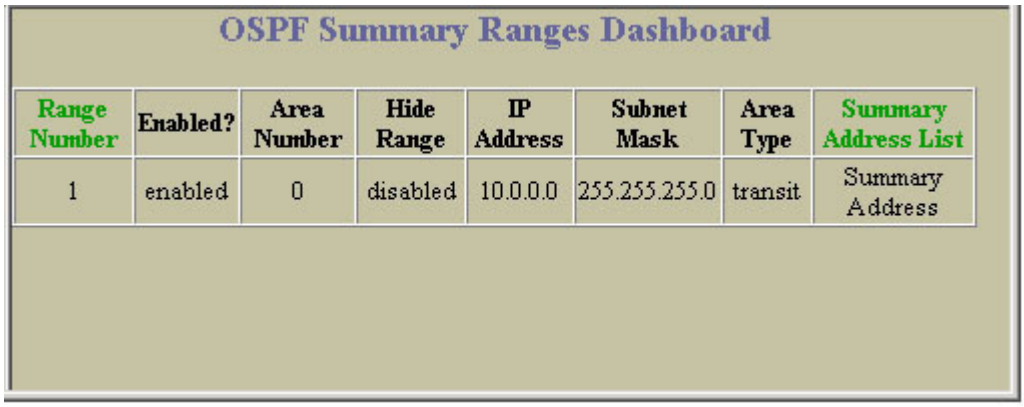
OSPF Areas Dashboard

Area Number	Area ID	Interface Count	LS Types	SPF Runs	LSA Count	ASBR Count	ABR Count	Total Neighbours	>=INIT	>=EXCH	=FULL
0	0.0.0.0	1	1 2 3 4 5	1	4	2	1	1	1	1	1

Select an area number to view statistics for the OSPF area.

OSPF Summary Ranges Dashboard

To display the following form, select **Layer 3 > OSPF > Summary Ranges** (click the underlined text, not the folder).



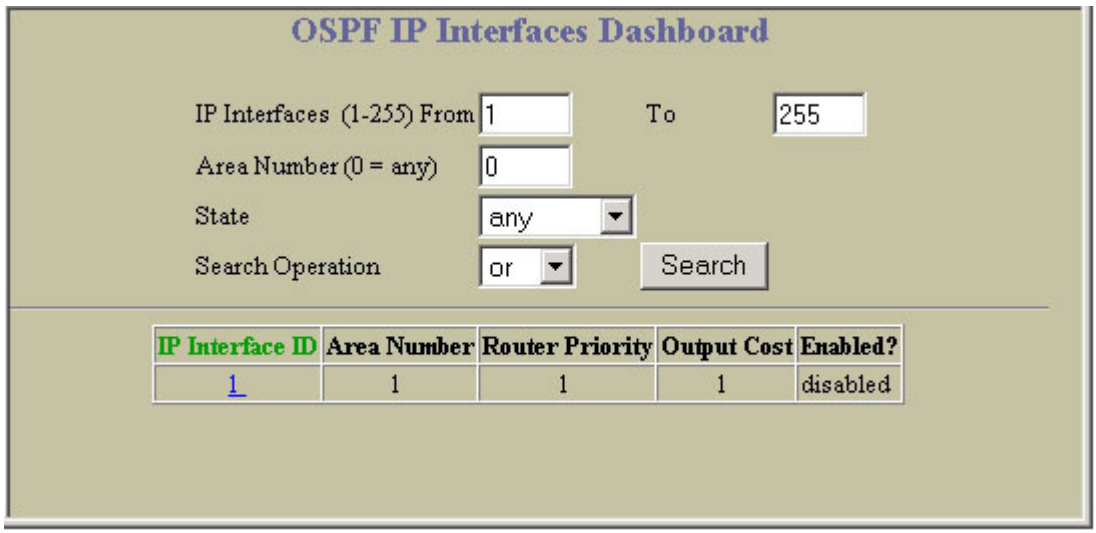
The following table describes the OSPF Summary Ranges Dashboard controls:

Table 33 OSPF Summary Ranges Dashboard controls

Control	Description
Range Number	Displays the summary range number.
Enabled?	Displays the status of the summary range, either **Enabled** or **Disabled**.
Area Number	Displays the area index associated with the summary range.
Hide Range	Indicates whether the summary range is hidden.
IP Address	Displays the base IP address for the summary range.
Subnet Mask	Displays the base subnet mask for the summary range.
Area Type	Display the area type associated with the summary range.
Summary Address List	Displays the summary address list for the range.

OSPF IP Interfaces Dashboard

To display the following form, select **Layer 3 > OSPF > OSPF Interfaces** (click the underlined text, not the folder).



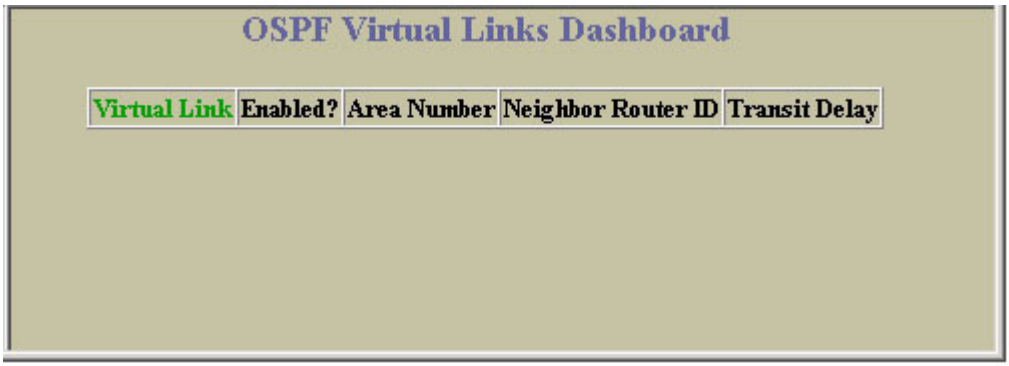
The following table describes the OSPF IP Interfaces Dashboard controls. Select an IP Interface ID number to view statistics for the interface.

Table 34 OSPF IP Interfaces Dashboard controls

Control	Description
Search Operation	To focus the search for an OSPF interface, enter search parameters: • IP interfaces • Area number • State Fields that have a value of "any" are ignored during the search. Choose a search operation: • **or**: Search for OSPF interfaces specified in the Search range that meet any of the criteria entered. • **and**: Search for OSPF interfaces specified in the Search range that meet all of the criteria entered. Click **Search** to display OSPF interfaces that fit the range and meet the criteria entered.

OSPF Virtual Links Dashboard

To display the following form, select **Layer 3 > OSPF > Virtual Links** (click the underlined text, not the folder).



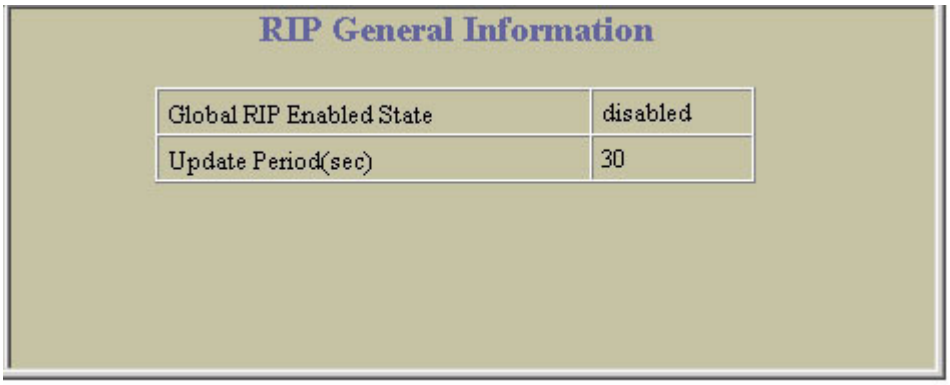
The following table describes the OSPF Virtual Links Dashboard controls:

Table 35 OSPF Virtual Links Dashboard controls

Control	Description
Virtual Link	Displays the virtual link number.
Enabled?	Displays the status of the virtual link, either **Enabled** or **Disabled**.
Area Number	Displays the area number associated with the virtual link.
Neighbor Router ID	Displays the neighbor router ID.
Transit Delay	Displays the transit delay value, in seconds.

RIP General Information

To display the following form, select **Layer 3 > RIP > General**.



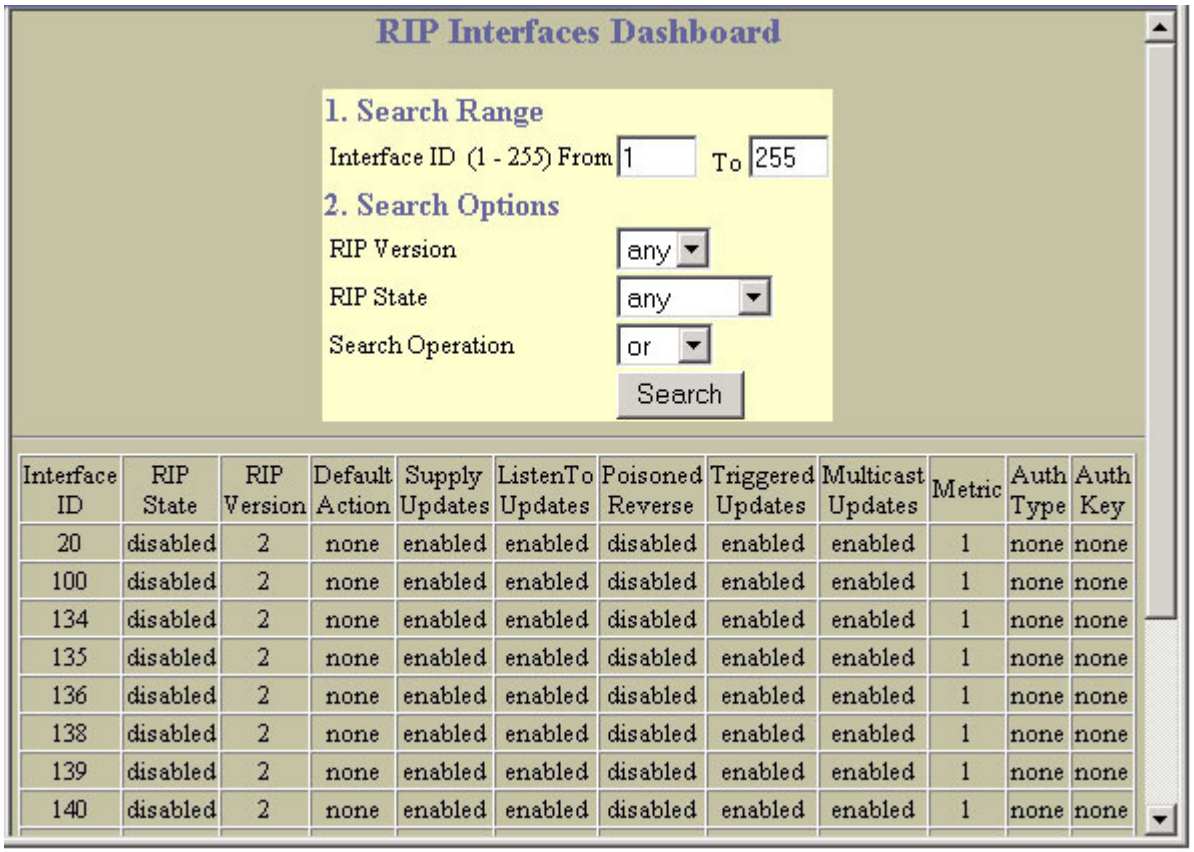
The following table describes the Routing Information Protocol (RIP) General Information controls:

Table 36 RIP General Information controls

Control	Description
Global RIP Enabled State	Displays the global state of RIP: **enabled** or **disabled**.
Update Period (sec)	Displays the time interval for sending for RIP table updates.

RIP Interfaces Dashboard

To display the following form, select **Layer 3 > RIP > RIP Interfaces** (click the underlined text, not the folder).



Interface ID	RIP State	RIP Version	Default Action	Supply Updates	ListenTo Updates	Poisoned Reverse	Triggered Updates	Multicast Updates	Metric	Auth Type	Auth Key
20	disabled	2	none	enabled	enabled	disabled	enabled	enabled	1	none	none
100	disabled	2	none	enabled	enabled	disabled	enabled	enabled	1	none	none
134	disabled	2	none	enabled	enabled	disabled	enabled	enabled	1	none	none
135	disabled	2	none	enabled	enabled	disabled	enabled	enabled	1	none	none
136	disabled	2	none	enabled	enabled	disabled	enabled	enabled	1	none	none
138	disabled	2	none	enabled	enabled	disabled	enabled	enabled	1	none	none
139	disabled	2	none	enabled	enabled	disabled	enabled	enabled	1	none	none
140	disabled	2	none	enabled	enabled	disabled	enabled	enabled	1	none	none

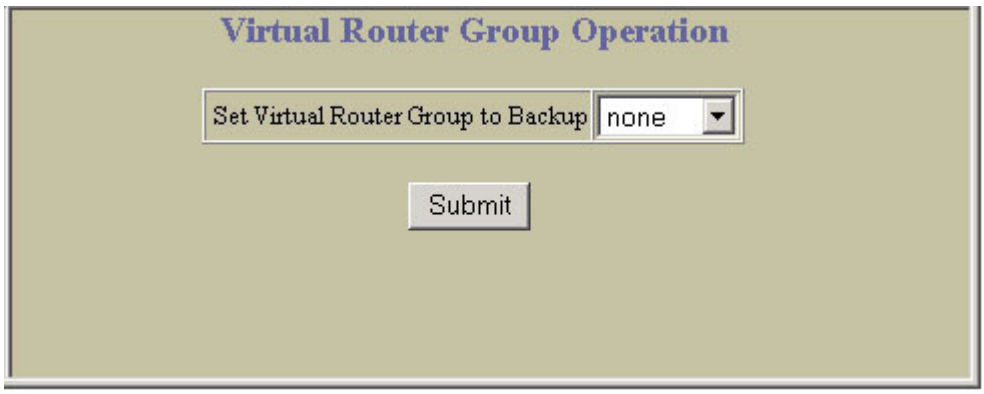
The following table describes the RIP Interfaces Dashboard controls:

Table 37 RIP Interfaces Dashboard controls

Control	Description
Search Range	To search for a RIP interface, enter a range of interface ID numbers in the **From** and **To** fields.
Search Options	To focus the search for a RIP interface, enter optional search parameters: • RIP version • RIP state Fields that have a value of "any" are ignored during the search. Choose a search operation: • **or**: Search for RIP interface specified in the search range that meet any of the criteria entered. • **and**: Search for RIP interface specified in the search range that meet all of the criteria entered. Click **Search** to display RIP interface that fit the range and meet the criteria entered.
Interface ID	Displays each interface number.
RIP State	Displays the current status of RIP in the interface: **enabled** or **disabled**.
RIP Version	Displays the RIP version used by the interface.
Default Action	Displays the default action for RIP on the interface.
Supply Updates	Displays the current status of Supply: **enabled** or **disabled**.
Listen to Updates	Displays whether Supply Updates is **enabled** or **disabled**.
Poisoned Reverse	Displays whether Poisoned Reverse is **enabled** or **disabled**.
Triggered Updates	Displays whether Triggered Updates is **enabled** or **disabled**.
Multicast Updates	Displays whether Multicast Updates is **enabled** or **disabled**.
Metric	Displays the route metric for the interface.
Auth Type	Displays the authentication type for the interface.
Auth Key	Displays the authentication key for the interface.

Virtual Router Group Operation

To display the following form, select **Layer 3 > VRRP > General**.



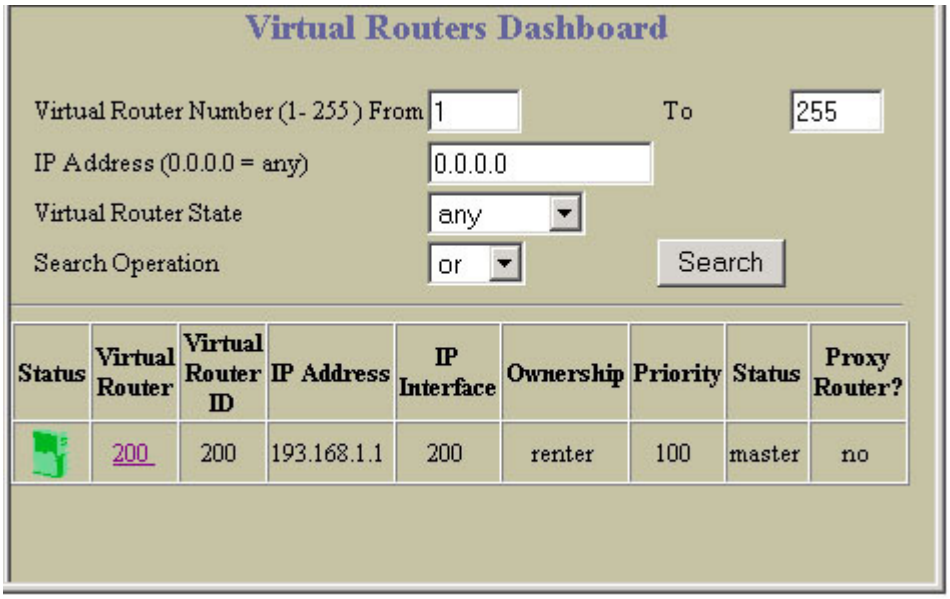
The following table describes the VRRP General controls:

Table 38 Virtual Router Group Operation controls

Control	Description
Set Virtual Router Group to Backup	Forces the master virtual router group into backup mode. This is generally used for passing master control back to a preferred switch once the preferred switch has been returned to service after a failure. When this command is executed, the current master gives up control and initiates a new election by temporarily advertising its own priority level as 0 (lowest). After the new election, the virtual router forced into backup mode by this command will resume master control in the following cases: • This switch owns the virtual router (the IP addresses of the virtual router and its IP interface are the same) • This switch's virtual router has a higher priority and preemption is enabled. • There are no other virtual routers available to take master control.

Virtual Routers Dashboard

To display the following form, select **Layer 3 > VRRP > Virtual Routers** (click the underlined text, not the folder).



The following table describes the Virtual Routers Dashboard controls:

Table 39 Virtual Routers Dashboard controls

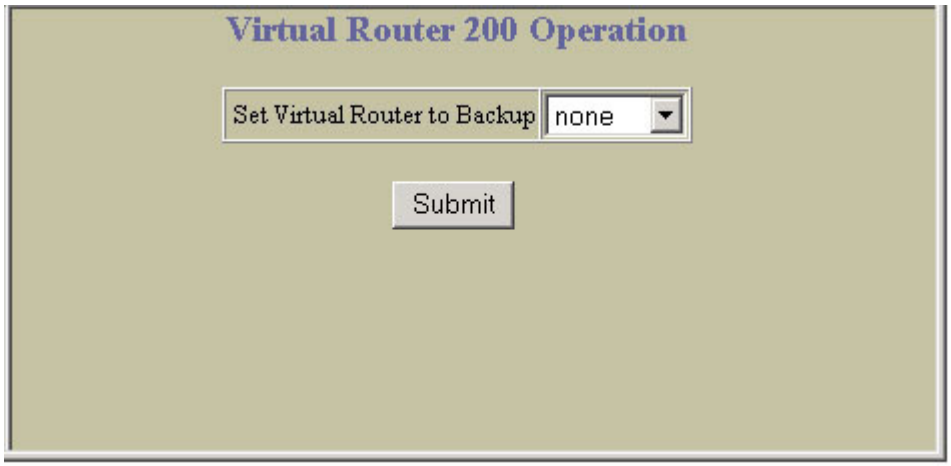
Control	Description
Search Operation	To focus the search for virtual routers, enter search parameters: • Virtual Router number • IP address • Virtual Router state Fields that have a value of "any" are ignored during the search. Choose a search operation: • **or**: Search for virtual routers specified in the Search range that meet any of the criteria entered. • **and**: Search for virtual routers specified in the Search range that meet all of the criteria entered. Click **Search** to display virtual routers that fit the range and meet the criteria entered.
Status	Shows whether the virtual router is **enabled** (green) or **disabled** (red).
Virtual Router	Displays the virtual router number for each virtual router.
Virtual Router ID	Displays the virtual router ID number for each virtual router.
IP Address	Displays the IP address of the virtual router.
IP Interface	Displays the IP interface associated with the virtual router.

Table 39 Virtual Routers Dashboard controls

Control	Description
Ownership	Displays the ownership status of the virtual router: **owner** or **renter**
Priority	Displays the priority number.
Status	Displays whether the virtual router is acting as master or standby.
Proxy Router	Shows the status of the virtual router as a proxy router: **yes** or **no**.

Virtual Router Operation

To display the following form, go to the Virtual Routers Dashboard. Select a virtual router number.



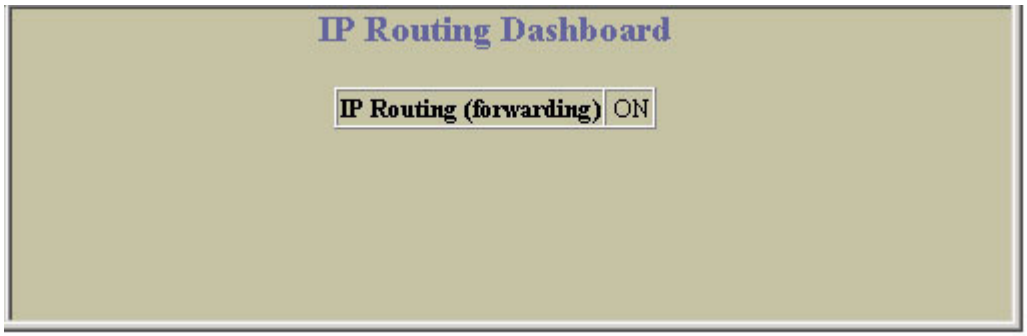
The following table describes the Virtual Router Operation controls:

Table 40 Virtual Router Operation controls

Control	Description
Set Virtual Router to Backup	Forces the master virtual router into backup mode. This is generally used for passing master control back to a preferred switch once the preferred switch has been returned to service after a failure. When this command is executed, the current master gives up control and initiates a new election by temporarily advertising its own priority level as 0 (lowest). After the new election, the virtual router forced into backup mode by this command will resume master control in the following cases: • This switch owns the virtual router (the IP addresses of the virtual router and its IP interface are the same) • This switch's virtual router has a higher priority and preemption is enabled. • There are no other virtual routers available to take master control.

IP Routing Dashboard

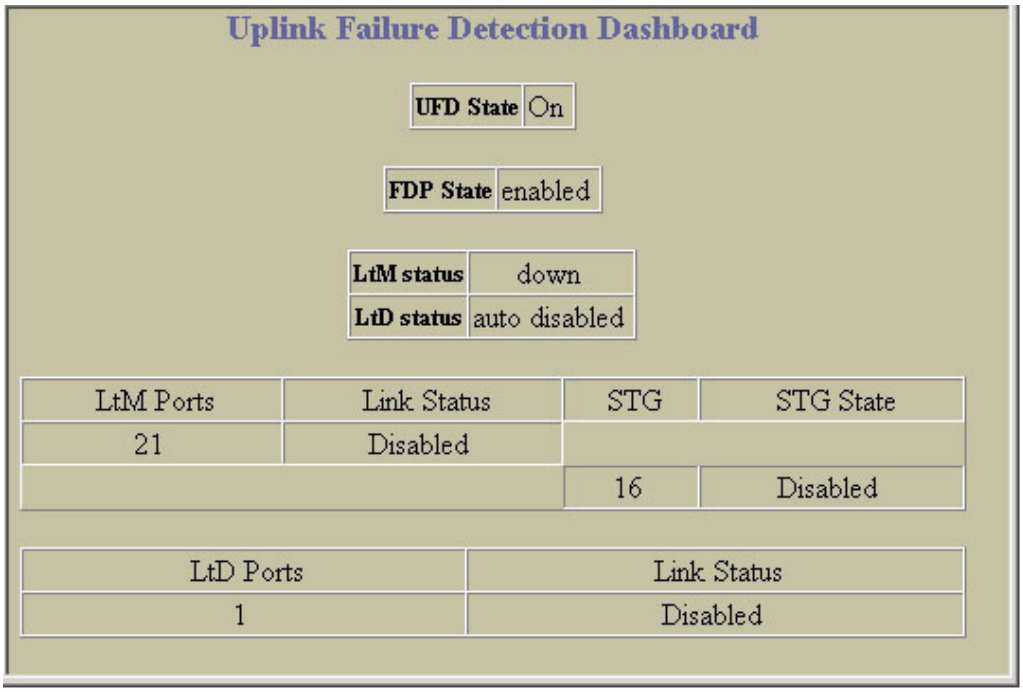
To display the following form, select **Layer 3 > General.**



This form summarizes IP Routing information.

Uplink Failure Detection Dashboard

To display the following form, select **Uplink Failure Detection** (click the underlined text, not the folder).



The following table describes the Uplink Failure Detection Dashboard controls:

Table 41 Uplink Failure Detection Dashboard controls

Control	Description
UFD State	Displays the global status of Uplink Failure Detection.
FDP State	Displays whether the Failure Detection Pair is **enabled** or **disabled**.
LtM status	Displays the current status of the Link to Monitor (LtM).
LtD status	Displays the current status of the Link to Disable (LtD).
LtM Ports	Displays the link status and Spanning Tree information for each port in the LtM.
LtD Ports	Displays the link status for each port in the LtD.

Viewing statistics

Introduction

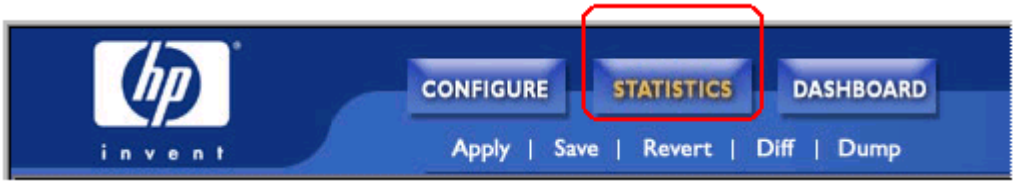
The GbE2 Interconnect Switch BBI can be used to view a variety of switch performance statistics. The same statistics that are available through the switch's command line interface are present on the BBI statistics forms.

The following provides a basic outline for viewing statistics. You should first be familiar with configuration as covered in the *HP ProLiant BL p-Class GbE2 Interconnect Switch Command Reference Guide*.

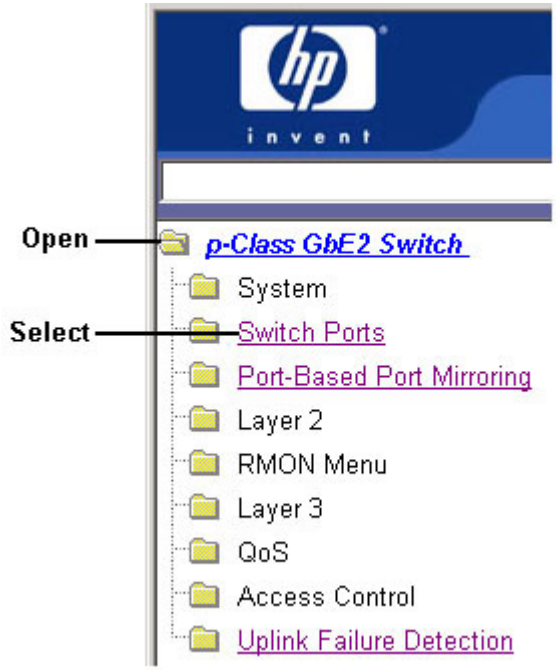
Steps for displaying statistics

Follow these basic steps for viewing GbE2 Interconnect Switch statistics.

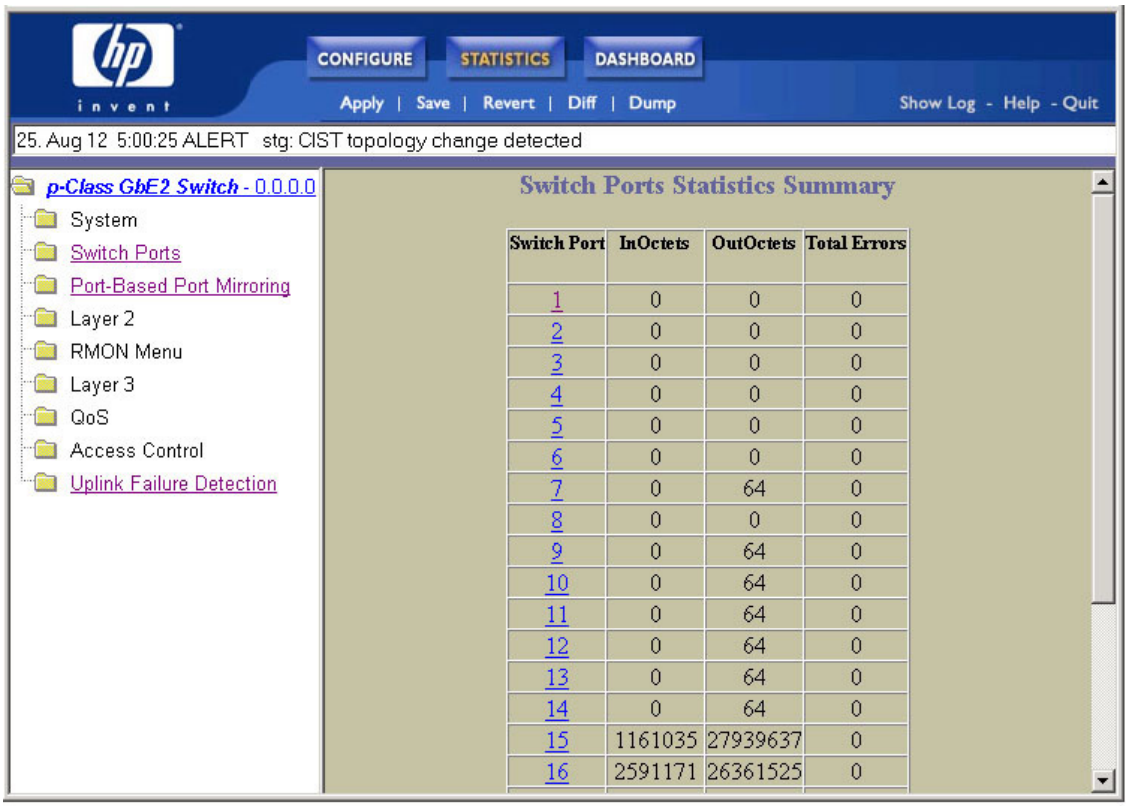
1. Select the **Statistics** context button in the toolbar.



2. Select a feature icon in the navigation window. For example, open the Switch folder and select **Switch Ports**.



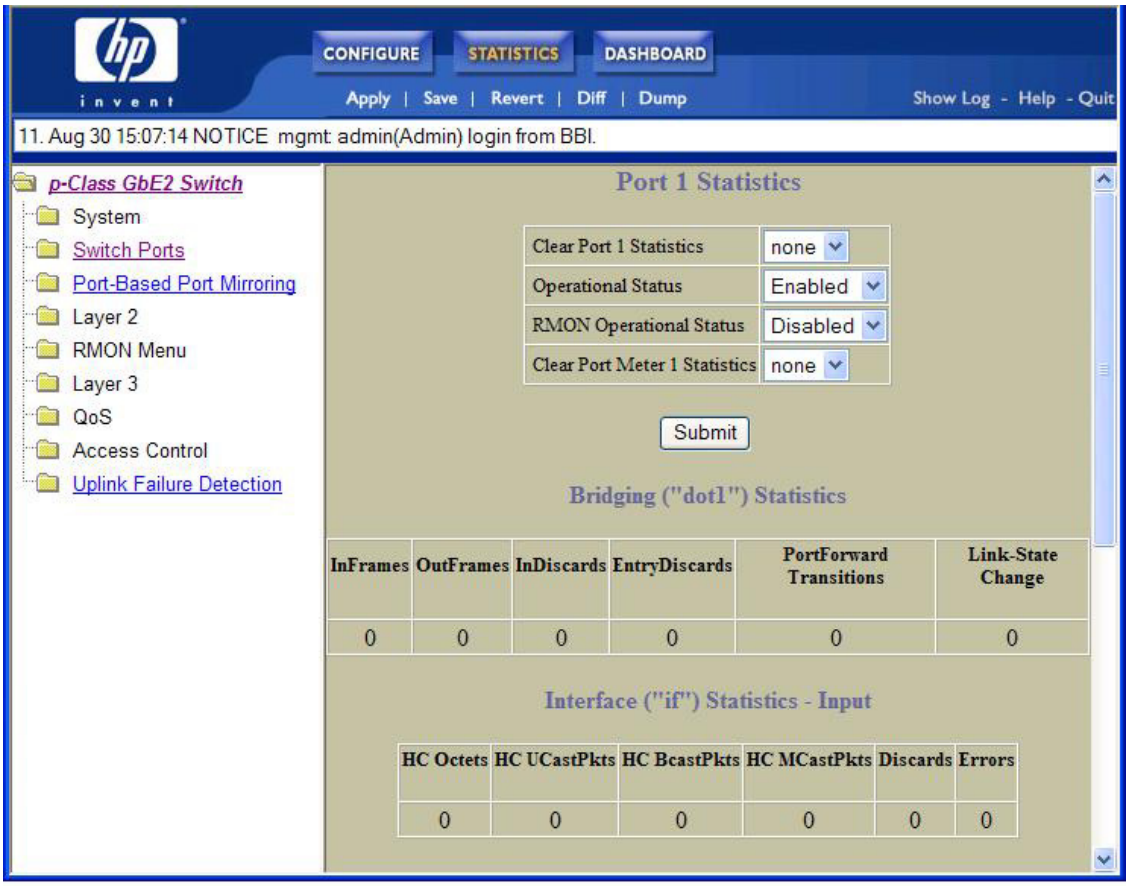
3. View the statistics in the forms window. For example:



Switch Port	InOctets	OutOctets	Total Errors
1	0	0	0
2	0	0	0
3	0	0	0
4	0	0	0
5	0	0	0
6	0	0	0
7	0	64	0
8	0	0	0
9	0	64	0
10	0	64	0
11	0	64	0
12	0	64	0
13	0	64	0
14	0	64	0
15	1161035	27939637	0
16	2591171	26361525	0

NOTE: Items that load other forms when selected are underlined.

4. Select an underlined item to view details on a per port basis. For example:



InFrames	OutFrames	InDiscards	EntryDiscards	PortForward Transitions	Link-State Change
0	0	0	0	0	0

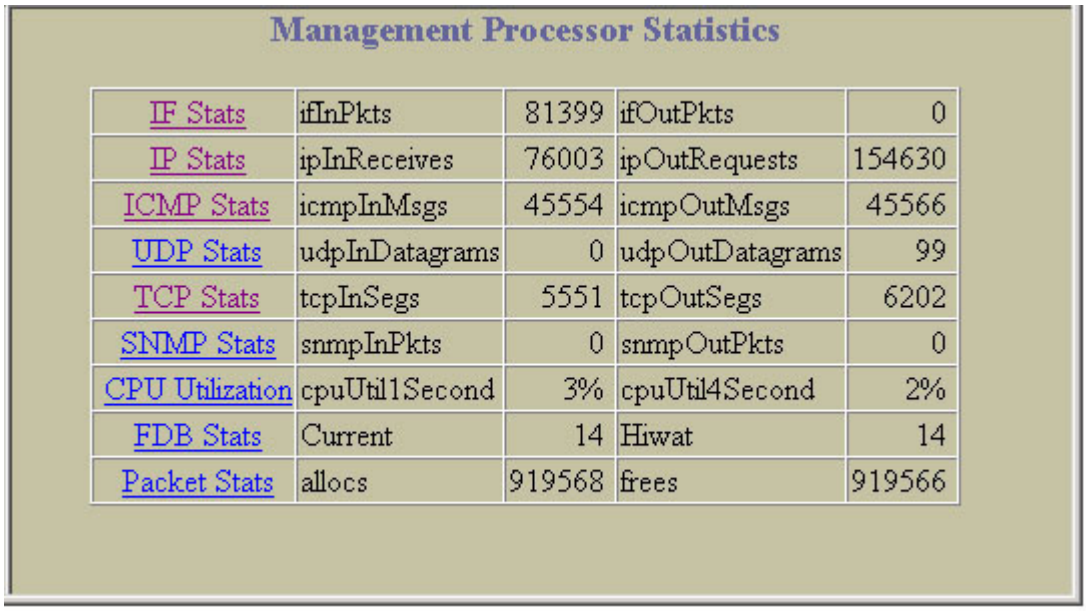
Interface ("if") Statistics - Input

HC Octets	HC UCastPkts	HC BcastPkts	HC MCastPkts	Discards	Errors
0	0	0	0	0	0

NOTE: This page is refreshed every 5 seconds.

Management Processor Statistics

To display the following form, select **System > General**.



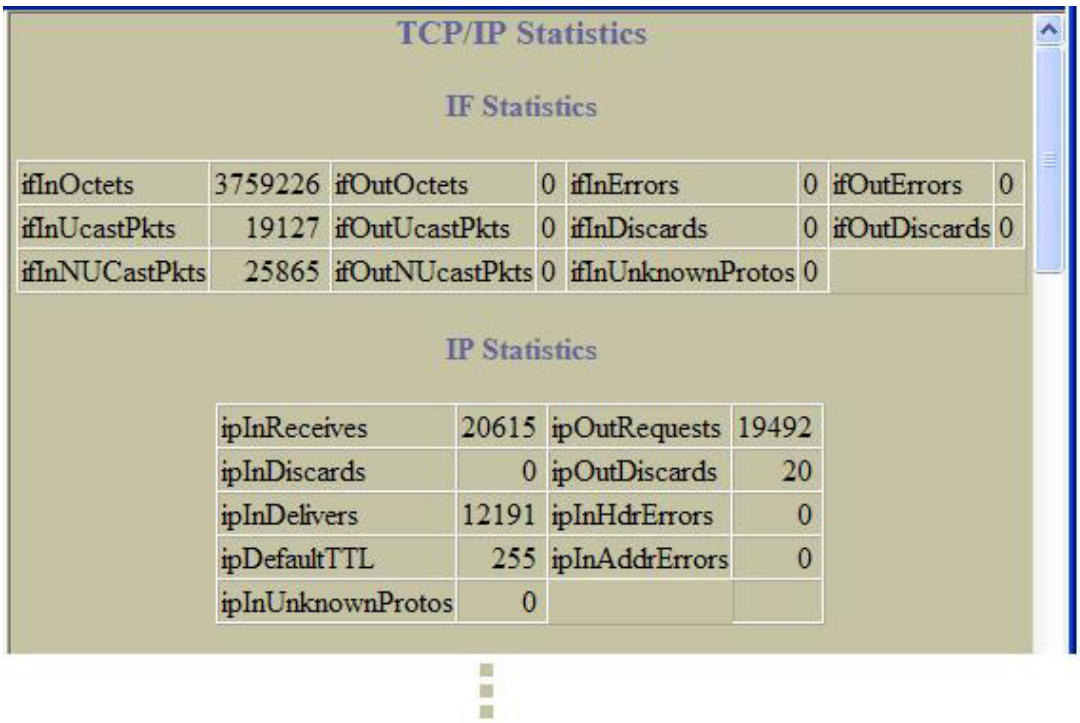
Management processor statistics are described in the following table:

Table 42 Management Processor Statistics

Statistic	Syntax and Usage
IF Stats	Click IF Stats to display IF portion of TCP/IP statistics
IP Stats	Click IP Stats to display IP portion of TCP/IP statistics.
ICMP Stats	Click ICMP Stats to display ICMP portion of TCP/IP statistics.
UDP Stats	Click UDP Stats to display UDP/SNMP statistics.
TCP Stats	Click TCP Stats to display TCP portion of TCP/IP statistics.
SNMP Stats	Click SNMP Stats to display UDP/SNMP statistics.
CPU Utilization	Click CPU Utilization to display CPU utilization.
FDB Stats	Click FDB Stats to display FDB statistics.
Packet Stats	Click Packet Stats to display MP Packet allocation statistics.

TCP/IP Statistics (IF and IP Statistics)

To display the following form, go to the Management Processor Statistics form. Select one of the following: **IF Stats**, **IP Stats**, **ICMP Stats**, or **TCP Stats**.



The following table describes the interface statistics:

Table 43 IF statistics

Statistics	Description
ifInOctets	The total number of octets received on the interface, including framing characters.
ifInUcastPkts	The number of packets, delivered by this sublayer to a higher sublayer, which were not addressed to a multicast or broadcast address at this sublayer.
ifInNUCastPkts	The number of packets, delivered by this sublayer to a higher sublayer, which were addressed to a multicast or broadcast address at this sublayer. This object is deprecated in favor of ifInMulticastPkts and ifInBroadcastPkts.
ifInDiscards	The number of inbound packets that were chosen to be discarded even though no errors were detected to prevent their being delivered to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
ifInErrors	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.
ifInUnknownProtos	For packet-oriented interfaces, the number of packets received via the interfaces that were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces which support protocol multiplexing the number of transmission units received via the interface which were discarded because of an unknown or unsupported protocol. For any interface that does not support protocol multiplexing, this counter will always be zero (0).
ifOutOctets	The total number of octets transmitted out of the interface, including framing characters.
ifOutUcastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were not addressed to a multicast or broadcast address at this sublayer, including those that were discarded or not sent.

Table 43 IF statistics

Statistics	Description
ifOutNUcastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a multicast or broadcast address at this sublayer, including those that were discarded or not sent. This object is deprecated in favor of ifOutMulticastPkts and ifOutBroadcastPkts.
ifOutDiscards	The number of outbound packets, which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
ifOutErrors	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.
ifStateChanges	The number of times an interface has transitioned from either down to up or from up to down.

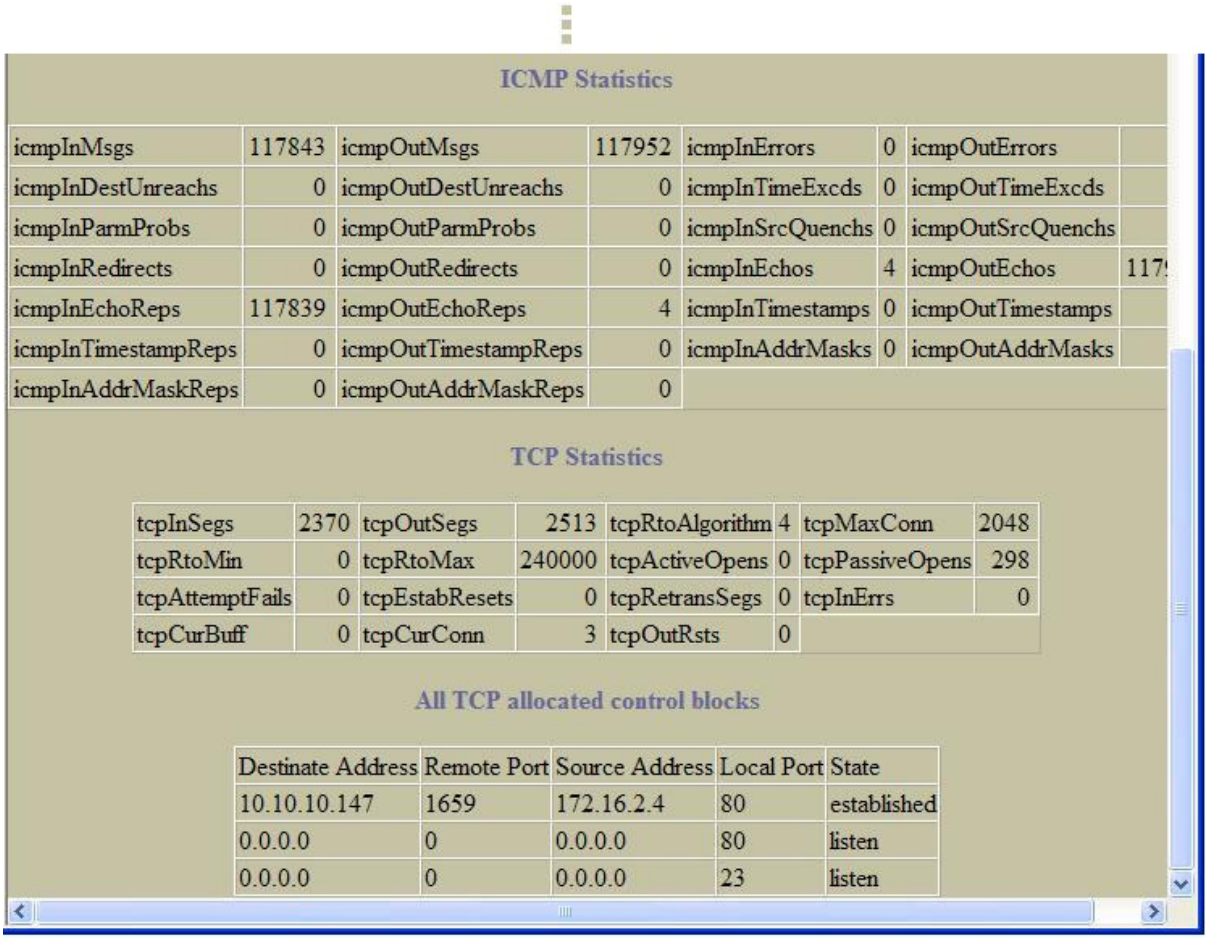
IP statistics are described in the following table:

Table 44 IP Statistics

Statistic	Description
ipInReceives	The total number of input datagrams received from interfaces, including those received in error.
ipOutRequests	The total number of IP datagrams which local IP user protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in `ipForwDatagrams`.
ipInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
ipOutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space). Note that this counter would include datagrams counted in `ipForwDatagrams` if any such packets met this (discretionary) discard criterion.
ipInDelivers	The total number of input datagrams successfully delivered to IP user protocols (including ICMP).
ipInHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad `checksums`, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so forth.
ipDefaultTTL	The default value inserted into the `Time-To-Live` (TTL) field of the IP header of datagrams originated at this entity (the switch), whenever a TTL value is not supplied by the transport layer protocol.
ipInAddrErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch). This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
ipInUnknownProtos	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.

TCP/IP Statistics (ICMP and IP TCP Statistics)

To display the following form, go to the Management Processor Statistics form. Select one of the following: **IF Stats**, **IP Stats**, **ICMP Stats**, or **TCP Stats**.



ICMP Statistics

icmpInMsgs	117843	icmpOutMsgs	117952	icmpInErrors	0	icmpOutErrors	
icmpInDestUnreachs	0	icmpOutDestUnreachs	0	icmpInTimeExcds	0	icmpOutTimeExcds	
icmpInParmProbs	0	icmpOutParmProbs	0	icmpInSrcQuenchs	0	icmpOutSrcQuenchs	
icmpInRedirects	0	icmpOutRedirects	0	icmpInEchos	4	icmpOutEchos	117
icmpInEchoReps	117839	icmpOutEchoReps	4	icmpInTimestamps	0	icmpOutTimestamps	
icmpInTimestampReps	0	icmpOutTimestampReps	0	icmpInAddrMasks	0	icmpOutAddrMasks	
icmpInAddrMaskReps	0	icmpOutAddrMaskReps	0				

TCP Statistics

tcpInSegs	2370	tcpOutSegs	2513	tcpRtoAlgorithm	4	tcpMaxConn	2048
tcpRtoMin	0	tcpRtoMax	240000	tcpActiveOpens	0	tcpPassiveOpens	298
tcpAttemptFails	0	tcpEstabResets	0	tcpRetransSegs	0	tcpInErrs	0
tcpCurBuff	0	tcpCurConn	3	tcpOutRsts	0		

All TCP allocated control blocks

Destinate Address	Remote Port	Source Address	Local Port	State
10.10.10.147	1659	172.16.2.4	80	established
0.0.0.0	0	0.0.0.0	80	listen
0.0.0.0	0	0.0.0.0	23	listen

ICMP statistics are described in the following table:

Table 45 ICMP Statistics

Statistic	Description
icmpInMsgs	The total number of ICMP messages which the entity (the switch) received. Note that this counter includes all those counted by `icmpInErrors`.
icmpOutMsgs	The total number of ICMP messages which this entity (the switch) attempted to send. Note that this counter includes all those counted by `icmpOutErrors`.
icmpInErrors	The number of ICMP messages that the entity (the switch) received but determined as having ICMP-specific errors (bad ICMP `checksums`, bad length, and so forth).
icmpOutErrors	The number of ICMP messages which this entity (the switch) did not send due to problems discovered within ICMP such as a lack of buffer. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of errors that contribute to this counter's value.
icmpInDestUnreachs	The number of ICMP Destination Unreachable messages received.
icmpOutDestUnreachs	The number of ICMP Destination Unreachable messages sent.
icmpInTimeExcds	The number of ICMP Time Exceeded messages received.
icmpOutTimeExcds	The number of ICMP Time Exceeded messages sent.
icmpInParmProbs	The number of ICMP Parameter Problem messages received.
icmpOutParmProbs	The number of ICMP Parameter Problem messages sent.

Table 45 ICMP Statistics

Statistic	Description
icmpInSrcQuenchs	The number of ICMP Source Quench (buffer almost full, stop sending data) messages received.
icmpOutSrcQuenchs	The number of ICMP Source Quench (buffer almost full, stop sending data) messages sent.
icmpInRedirects	The number of ICMP Redirect messages received.
icmpOutRedirects	The number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
icmpInEchos	The number of ICMP Echo (request) messages received.
icmpOutEchos	The number of ICMP Echo (request) messages sent.
icmpInEchoReps	The number of ICMP Echo Reply messages received.
icmpOutEchoReps	The number of ICMP Echo Reply messages sent.
icmpInTimestamps	The number of ICMP Timestamp (request) messages received.
icmpOutTimestamps	The number of ICMP Timestamp (request) messages sent.
icmpInTimestampReps	The number of ICMP Timestamp `Reply` messages received.
icmpOutTimestampReps	The number of ICMP Timestamp `Reply` messages sent.
icmpInAddrMasks	The number of ICMP Address Mask Request messages received.
icmpOutAddrMasks	The number of ICMP Address Mask Request messages sent.
icmpInAddrMaskReps	The number of ICMP Address Mask Reply messages received.
icmpOutAddrMaskReps	The number of ICMP Address Mask Reply messages sent.

TCP statistics are described in the following table:

Table 46 TCP Statistics

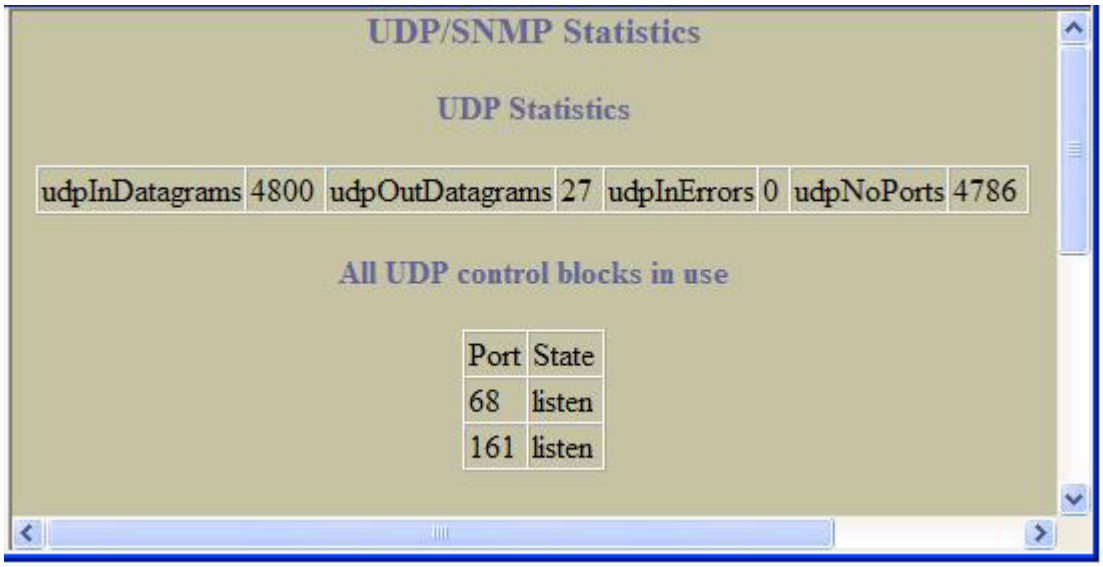
Statistic	Description
tcpInSegs	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
tcpOutSegs	The total number of segments sent, including those on current connections, but excluding those containing only retransmitted octets.
tcpRtoAlgorithm	The algorithm used to determine the timeout value used for retransmitting unacknowledged octets.
tcpMaxConn	The limit on the total number of TCP connections the entity (the switch) can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.
tcpRtoMin	The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the LBOUND quantity described in RFC 793.
tcpRtoMax	The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the UBOUND quantity described in RFC 793.
tcpActiveOpens	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
tcpPassiveOpens	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.

Table 46 TCP Statistics

Statistic	Description
tcpAttemptFails	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYNRCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
tcpEstabResets	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
tcpRetransSegs	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
tcpInErrs	The total number of segments received in error (for example, bad TCP `checksums`).
tcpCurBuff	The total number of outstanding memory allocations from heap by TCP protocol stack.
tcpCurConn	The total number of outstanding TCP sessions that are currently opened.
tcpOutRsts	The number of TCP segments sent containing the RST flag.
All TCP allocated control blocks	
Destinate Address	Switch IP address of TCP connections.
Remote Port	TCP port used by the remote device.
Source Address	IP address of TCP source connections.
Local Port	Available TCP ports used for connecting to the switch.
State	State of each TCP connection.

UDP/SNMP Statistics

To display the following form, go to the Management Processor Statistics form. Select **UDP Stats** or **SNMP Stats**.

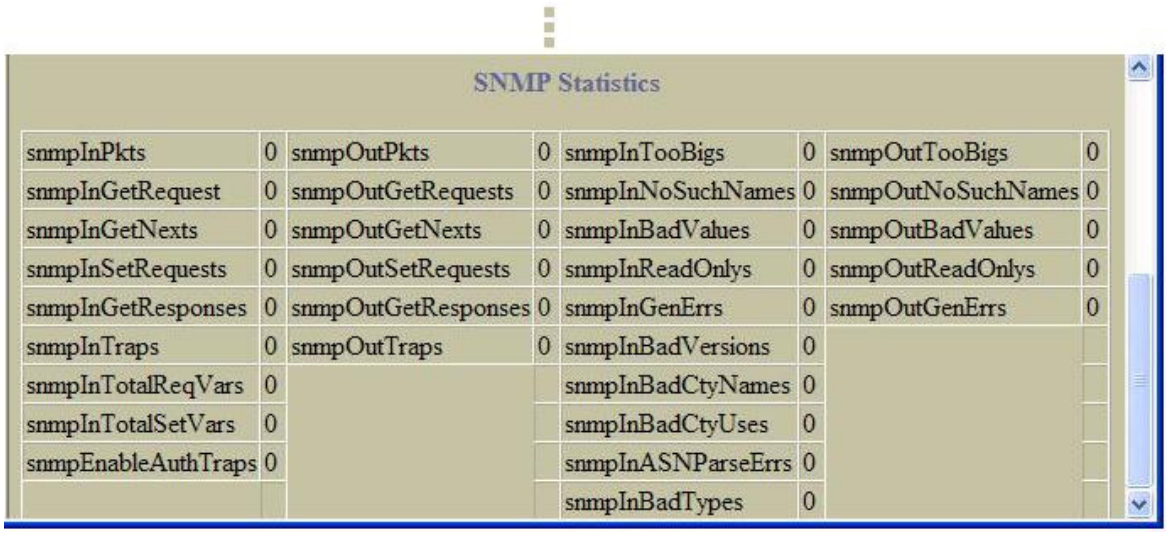


UDP statistics are described in the following table:

Table 47 UDP Statistics

Statistic	Description
udpInDatagrams	The total number of UDP datagrams delivered to the switch.
udpOutDatagrams	The total number of UDP datagrams sent from this entity (the switch).
udpInErrors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
udpNoPorts	The total number of received UDP datagrams for which there was no application at the destination port.

To display the following form, go to the Management Processor Statistics form. Select **UDP Stats** or **SNMP Stats**, and scroll down.



SNMP statistics are described in the following table:

Table 48 SNMP Statistics

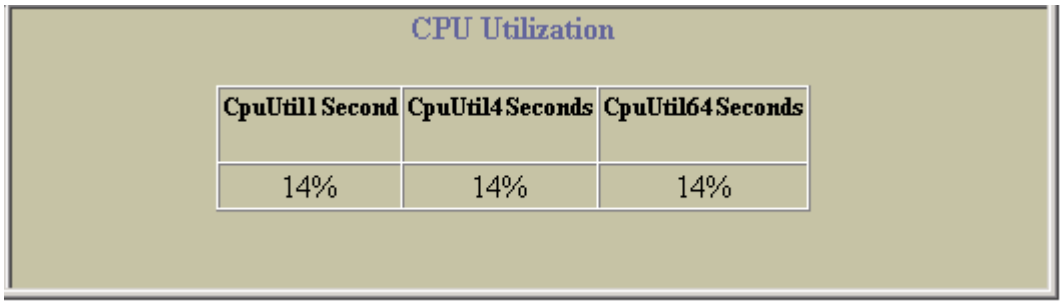
Statistic	Description
snmpInPkts	The total number of Messages delivered to the SNMP entity from the transport service.
snmpOutPkts	The total number of SNMP Messages that were passed from the SNMP protocol entity to the transport service.
snmpInTooBigs	The total number of SNMP Protocol Data Units (PDUs) that were delivered to the SNMP protocol entity and for which the value of the error-status field is too big.
snmpOutTooBigs	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is too big.
snmpInGetRequest	The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpOutGetRequests	The total number of SNMP Get-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpInNoSuchNames	The total number of SNMP Protocol Data Units (PDUs) that were delivered to the SNMP protocol entity and for which the value of the error-status field is `noSuchName`.
snmpOutNoSuchNames	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status is `noSuchName`.
snmpInGetNexts	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpOutGetNexts	The total number of SNMP Get-Next Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpInBadValues	The total number of SNMP Protocol Data Units (PDUs) that were delivered to the SNMP protocol entity and for which the value of the error-status field is `badValue`.
snmpOutBadValues	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is `badValue`.
snmpInSetRequests	The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpOutSetRequests	The total number of SNMP Set-Request Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.

Table 48 SNMP Statistics

Statistic	Description
snmpInReadOnlys	The total number of valid SNMP Protocol Data Units (PDUs), which were delivered to the SNMP protocol entity and for which the value of the error-status field is 'read-Only'. It should be noted that it is a protocol error to generate an SNMP PDU, which contains the value 'read-Only' in the error-status field. As such, this object is provided as a means of detecting incorrect implementations of the SNMP.
snmpOutReadOnlys	Not in use.
snmpInGetResponses	The total number of SNMP Get-Response Protocol Data Units (PDUs) that were delivered to the SNMP protocol entity.
snmpOutGetResponses	The total number of SNMP Get-Response Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpInGenErrs	The total number of SNMP Protocol Data Units (PDUs), which were delivered to the SNMP protocol entity and for which the value of the error-status field is `genErr`.
snmpOutGenErrs	The total number of SNMP Protocol Data Units (PDUs), which were generated by the SNMP protocol entity and for which the value of the error-status field is `genErr`.
snmpInTraps	The total number of SNMP Trap Protocol Data Units (PDUs), which have been accepted and processed by the SNMP protocol entity.
snmpOutTraps	The total number of SNMP Trap Protocol Data Units (PDUs), which have been generated by the SNMP protocol entity.
snmpInBadVersions	The total number of SNMP Messages, which were delivered to the SNMP protocol entity and were for an unsupported SNMP version.
snmpInTotalReqVars	The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as a result of receiving valid SNMP Get- Request and Get-Next Protocol Data Units (PDUs).
snmpInBadCtyNames	The total number of SNMP Messages delivered to the SNMP entity that used an SNMP community name not known to the said entity (the switch).
snmpInTotalSetVars	The total number of MIB objects, which have been altered successfully by the SNMP protocol entity as a result of receiving valid SNMP Set-Request Protocol Data Units (PDUs).
snmpInBadCtyUses	The total number of SNMP Messages delivered to the SNMP protocol entity that represented an SNMP operation that was not allowed by the SNMP community named in the Message.
snmpEnableAuthTraps	An object to enable or disable the authentication traps generated by this entity (the switch).
snmpInASNParseErrs	The total number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding SNMP Messages received. **Note:** OSI's method of specifying abstract objects is called ASN.1 (Abstract Syntax Notation One, defined in X.208), and one set of rules for representing such objects as strings of ones and zeros is called the BER (Basic Encoding Rules, defined in X.209). ASN.1 is a flexible notation that allows one to define a variety of data types, from simple types such as integers and bit strings to structured types such as sets and sequences. BER describes how to represent or encode values of each ASN.1 type as a string of eight-bit octets.
snmpInBadTypes	The total number of SNMP Messages which failed ASN parsing.

CPU Utilization

To display the following form, go to the Management Processor Statistics form. Select **CPU Utilization**.



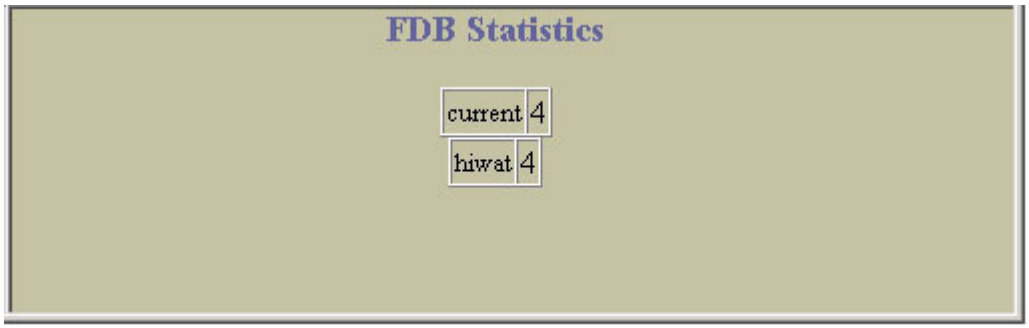
CPU statistics are described in the following table:

Table 49 CPU Statistics

Statistic	Description
CpuUtil1Second	The utilization of MP CPU over 1 second. It shows the percentage.
CpuUtil4Seconds	The utilization of MP CPU over 4 seconds. It shows the percentage.
CpuUtil64Seconds	The utilization of MP CPU over 64 seconds. It shows the percentage.

FDB Statistics

To display the following form, go to the Management Processor Statistics form. Select **FDB Stats**.



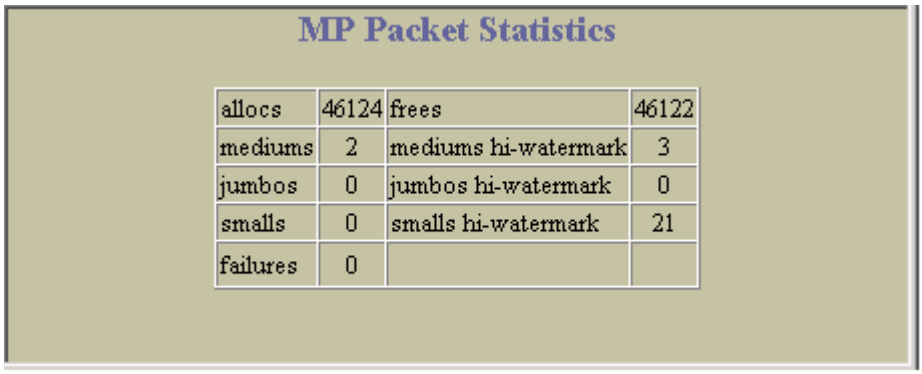
FDB statistics are described in the following table:

Table 50 Forwarding Database Statistics

Statistic	Description
current	Current number of entries in the Forwarding Database.
hiwat	Highest number of entries recorded at any given time in the Forwarding Database.

MP Packet Statistics

To display the following form, go to the Management Processor Statistics form. Select **Packet Stats**.



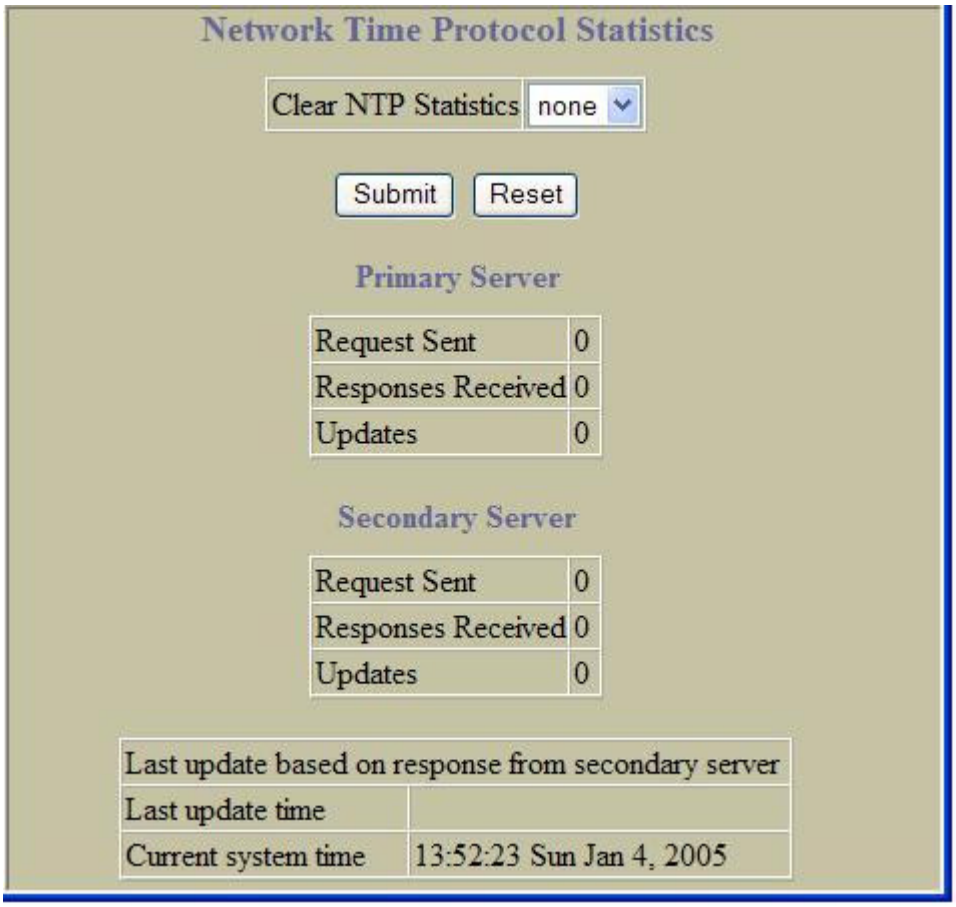
MP packet statistics are described in the following table:

Table 51 Packet Statistics

Statistic	Description
allocs	Total number of packet allocations from the packet buffer pool by the TCP/IP protocol stack.
frees	Total number of packets freed from the packet buffer pool by the TCP/IP protocol stack.
mediums	Total number of packet allocations with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
mediums hi-watermark	The highest number of packet allocation with size between 128 to 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
jumbos	Total number of packet allocations with size greater than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
jumbos hi-watermark	The highest number of packet allocation with size greater than 1536 bytes from the packet buffer pool by the TCP/IP protocol stack.
smalls	Total number of packet allocations with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack.
smalls hi-watermark	The highest number of packet allocation with size less than 128 bytes from the packet buffer pool by the TCP/IP protocol stack.
failures	Total number of packet allocation failures from the packet buffer pool by the TCP/IP protocol stack.

Network Time Protocol Statistics

To display the following form, select **System > NTP**.



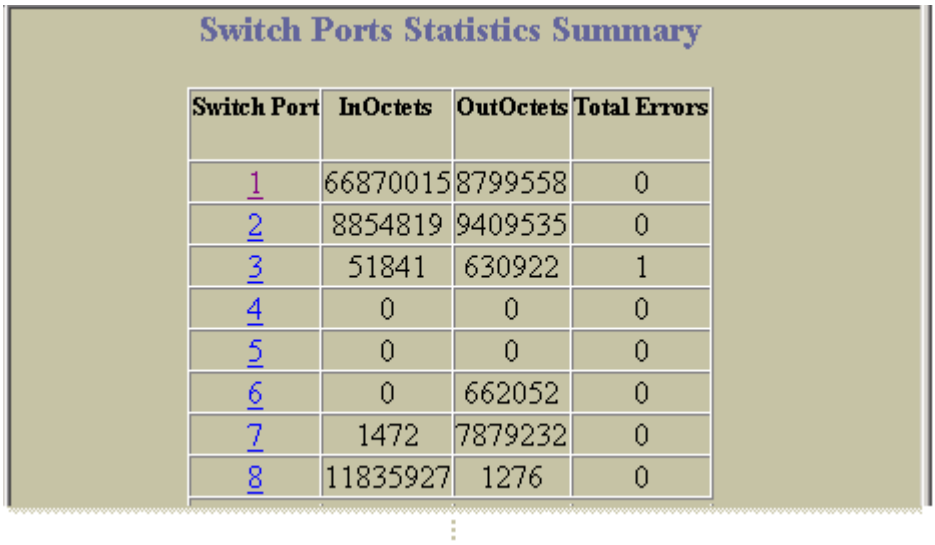
Network Time Protocol statistics for the primary and secondary NTP servers are described in the following table:

Table 52 NTP Statistics

Statistic	Description
Request Sent	The total number of NTP requests the switch sent to the primary NTP server to synchronize time.
Responses Received	The total number of NTP responses received from the primary NTP server.
Updates	The total number of times the switch updated its time based on the NTP responses received from the primary NTP server.
Last update time	The time stamp showing the time when the switch was last updated.
Current system time	The current switch system time.

Switch Ports Statistics Summary

To display the following form, select **Switch Ports** (click the underlined text, not the folder).



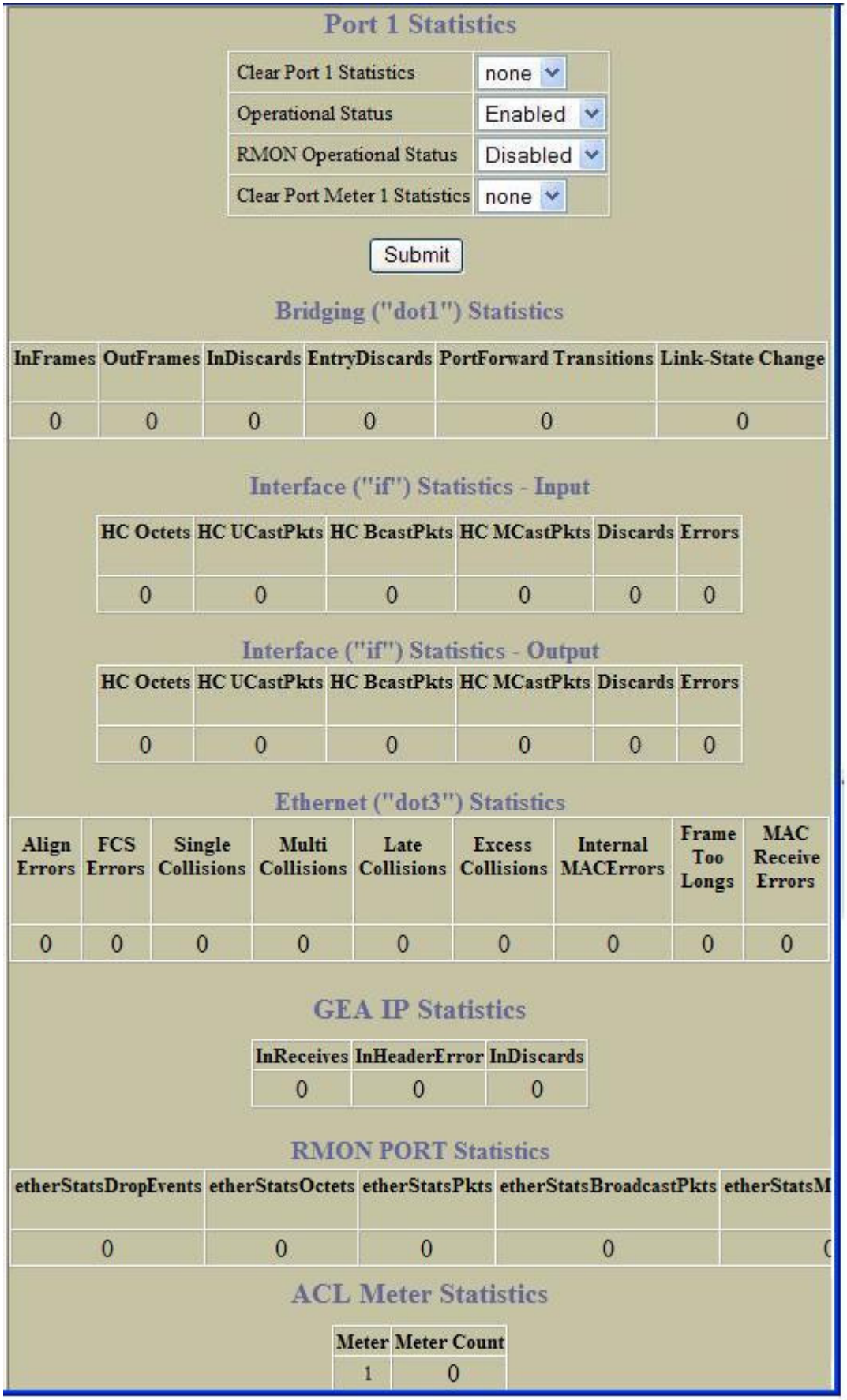
Switch Ports Statistics Summary

Switch Port	InOctets	OutOctets	Total Errors
1	66870015	8799558	0
2	8854819	9409535	0
3	51841	630922	1
4	0	0	0
5	0	0	0
6	0	662052	0
7	1472	7879232	0
8	11835927	1276	0

This form displays traffic statistics on a port-by-port basis. For more information, select a port number to display detailed statistics for that port.

Port Statistics

To display the following form, go to the Switch Ports Statistics Summary form. Select a Switch Port number.



Port 1 Statistics

Clear Port 1 Statistics	none
Operational Status	Enabled
RMON Operational Status	Disabled
Clear Port Meter 1 Statistics	none

Submit

Bridging ("dot1") Statistics

InFrames	OutFrames	InDiscards	EntryDiscards	PortForward Transitions	Link-State Change
0	0	0	0	0	0

Interface ("if") Statistics - Input

HC Octets	HC UCastPkts	HC BcastPkts	HC MCastPkts	Discards	Errors
0	0	0	0	0	0

Interface ("if") Statistics - Output

HC Octets	HC UCastPkts	HC BcastPkts	HC MCastPkts	Discards	Errors
0	0	0	0	0	0

Ethernet ("dot3") Statistics

Align Errors	FCS Errors	Single Collisions	Multi Collisions	Late Collisions	Excess Collisions	Internal MACErrors	Frame Too Longs	MAC Receive Errors
0	0	0	0	0	0	0	0	0

GEA IP Statistics

InReceives	InHeaderError	InDiscards
0	0	0

RMON PORT Statistics

etherStatsDropEvents	etherStatsOctets	etherStatsPkts	etherStatsBroadcastPkts	etherStatsM
0	0	0	0	0

ACL Meter Statistics

Meter	Meter Count
1	0

Port statistics are described in the following table:

Table 53 Port Statistics

Control	Description
Clear Port x Statistics	Select **Clear** and click **Submit** to clear statistics for this port.
Operational Status	Enables or disables the port.
RMON Operational Status	Enables or disables RMON for the port.
Clear Port x Meter Statistics	Select **Clear** and click **Submit** to clear meter statistics for this port.

The next several tables contain specific information about bridging, interface (input and output), and Ethernet statistics.

Bridging ("dot1") Statistics

The following table describes the bridging statistics of the selected port:

Table 54 Bridging statistics of a port

Statistic	Description
InFrames	The number of frames that have been received by this port from its segment. A frame received on the interface corresponding to this port is only counted by this object if and only if it is for a protocol being processed by the local bridging function, including bridge management frames.
OutFrames	The number of frames that have been transmitted by this port to its segment. Note that a frame transmitted on the interface corresponding to this port is only counted by this object if and only if it is for a protocol being processed by the local bridging function, including bridge management frames.
InDiscards	Count of valid frames received that were discarded (that is, filtered) by the Forwarding Process.
EntryDiscards	The total number of Forwarding Database entries, which have been or would have been learnt, but have been discarded due to a lack of space to store them in the Forwarding Database. If this counter is increasing, it indicates that the Forwarding Database is regularly becoming full (a condition which has unpleasant performance effects on the sub network). If this counter has a significant value but is not presently increasing, it indicates that the problem has been occurring but is not persistent.
DelayExceed	The number of frames discarded by this port due to excessive transit delay through the bridge. It is incriminated by both transparent and source route bridges.
MtuExceed	The number of frames discarded by this port due to an excessive size. It is incremented by both transparent and source route bridges.
PortForward Transitions	The number of times this port has transitioned from the Learning state to the Forwarding state.
Link-State Change	The number of times an interface has transitioned from either down to up or from up to down.

Interface ("if") Statistics - Input

The following table describes the interface input statistics of the selected port:

Table 55 Interface Statistics for a Port - Input

Statistic	Description
HC Octets	The total number of octets received on the interface, including framing characters.
HC UCastPkts	The number of packets, delivered by this sub layer to a higher sub layer, which were not addressed to a multicast or broadcast address at this sub layer.
HC BcastPkts	The number of packets, delivered by this sub layer to a higher sub layer, which were addressed to a broadcast address at this sub layer.

Table 55 Interface Statistics for a Port - Input

Statistic	Description
HC MCastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a multicast address at this sub layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses.
Discards	The number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their being delivered to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Errors	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.

Interface ("if") Statistics - Output

The following table describes the interface output statistics of the selected port:

Table 56 Interface Statistics for a Port - Output

Statistic	Description
HC Octets	The total number of octets transmitted out of the interface, including framing characters.
HC UCastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were not addressed to a multicast or broadcast address at this sub layer, including those that were discarded or not sent.
HC BcastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a broadcast address at this sub layer, including those that were discarded or not sent. This object is a 64-bit version of `ifOutBroadcastPkts`
HC MCastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a multicast address at this sub layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses. This object is a 64-bit version of `ifOutMulticastPkts`.
Discards	The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Errors	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.

Ethernet ("dot3") Statistics

The following table describes the Ethernet statistics of the selected port:

Table 57 Ethernet Statistics for a Port

Statistic	Description
Align Errors	A count of frames received on a particular interface that is not an integral number of octets in length and do not pass the Frame Check Sequence (FCS) check. The count represented by an instance of this object is incremented when the `alignmentError` status is returned by the MAC service to the Logical Link Control (LLC) (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.

Table 57 Ethernet Statistics for a Port

Statistic	Description
FCS Errors	A count of frames received on a particular interface that is an integral number of octets in length but do not pass the Frame Check Sequence (FCS) check. The count represented by an instance of this object is incremented when the `frameCheckError` status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
Single Collisions	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of the `ifOutUcastPkts`, `ifOutMulticastPkts`, or `ifOutBroadcastPkts`, and is not counted by the corresponding instance of the `dot3StatsMultipleCollision-Frame` object.
Multi Collisions	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of the `ifOutUcastPkts`, `ifOutMulticastPkts`, or `ifOutBroadcastPkts`, and is not counted by the corresponding instance of the `dot3StatsSingleCollision-Frames` object.
Late Collisions	The number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mbit/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.
Excess Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions.
Internal MACErrors	A count of frames for which transmission on a particular interface fails due to an internal MAC sub layer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of the `dot3StatsLateCollisions` object, the `dot3StatsExcessiveCollisions` object, or the `dot3Stats-CarrierSenseErrors` object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface that are not otherwise counted.
Frame Too Longs	A count of frames received on a particular interface that exceeds the maximum permitted frame size. The count represented by an instance of this object is incremented when the `frameTooLong` status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
Mac Receive Errors	A count of frames for which reception on a particular interface fails due to an internal MAC sub layer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of the `dot3StatsFrameTooLongs` object, the `dot3Stats-AlignmentErrors` object, or the `dot3StatsFCSErrors` object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object may represent a count of received errors on a particular interface that are not otherwise counted.

GEA IP Statistics

The following table describes the GEA statistics for the selected port:

Table 58 GEA IP statistics of a port

Statistic	Description
InReceives	The total number of input datagrams received from interfaces, including those received in error.
InHeaderError	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch).
InDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.

ACL Meter Statistics

The following table describes the ACL Meter statistics for the selected port:

Table 59 ACL Meter statistics of a port

Statistic	Description
Meter	Displays port ACL meters.
Meter Count	Displays the number of times the meter was activated.

RMON Port Statistics

The following table describes the Remote Monitoring (RMON) statistics of the selected port:

Table 60 RMON Statistics

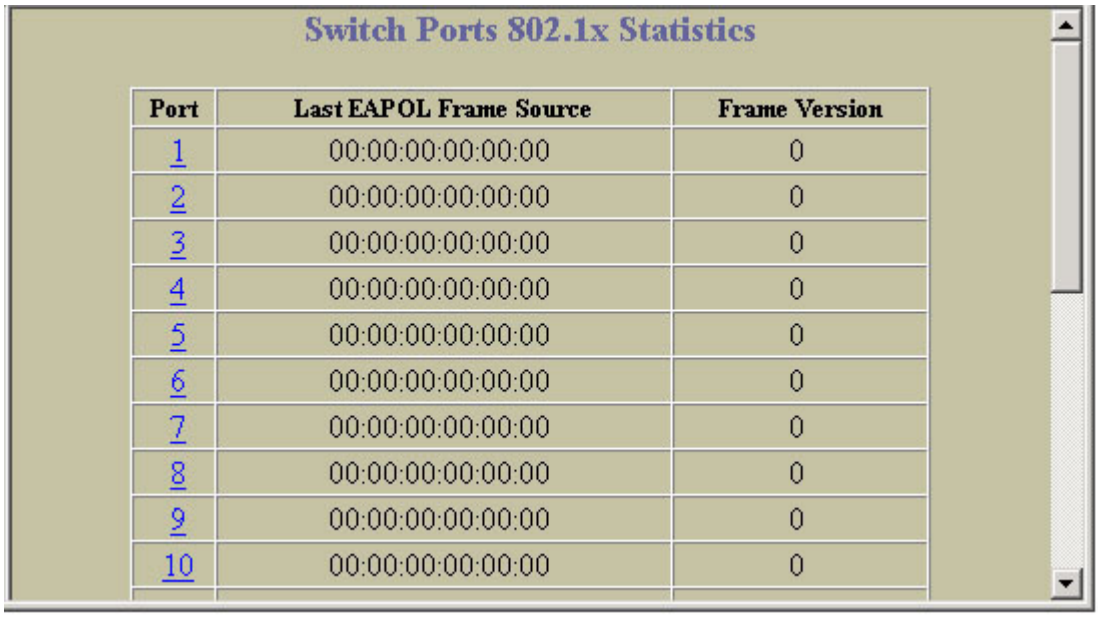
Statistic	Description
`etherStatsDropEvents`	The total number of packets received that were dropped because of system resource constraints.
`etherStatsOctets`	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
`etherStatsPkts`	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
`etherStatsBroadcastPkts`	The total number of good packets received that were directed to the broadcast address.
`etherStatsMulticastPkts`	The total number of good packets received that were directed to a multicast address.
`etherStatsCRCAlignErrors`	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
`etherStatsUndersizePkts`	The total number of packets received that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
`etherStatsOversizePkts`	The total number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed.

Table 60 RMON Statistics

Statistic	Description
etherStatsFragments	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
etherStatsJabbers	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Jabber is defined as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
etherStatsCollisions	The best estimate of the total number of collisions on this Ethernet segment.
etherStatsPkts64 Octets	The total number of packets (including bad packets) received that were less than or equal to 64 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts65to127 Octets	The total number of packets (including bad packets) received that were greater than 64 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts128to255 Octets	The total number of packets (including bad packets) received that were greater than 127 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts256to511 Octets	The total number of packets (including bad packets) received that were greater than 255 octets in length (excluding framing bits but including FCSoctets).
etherStatsPkts512to1023 Octets	The total number of packets (including bad packets) received that were greater than 511 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts1024to1518 Octets	The total number of packets (including bad packets) received that were greater than 1023 octets in length (excluding framing bits but including FCS octets).

Switch Ports 802.1x Statistics

To display the following form, select **Layer 2 > 802.1x > Switch Ports**.



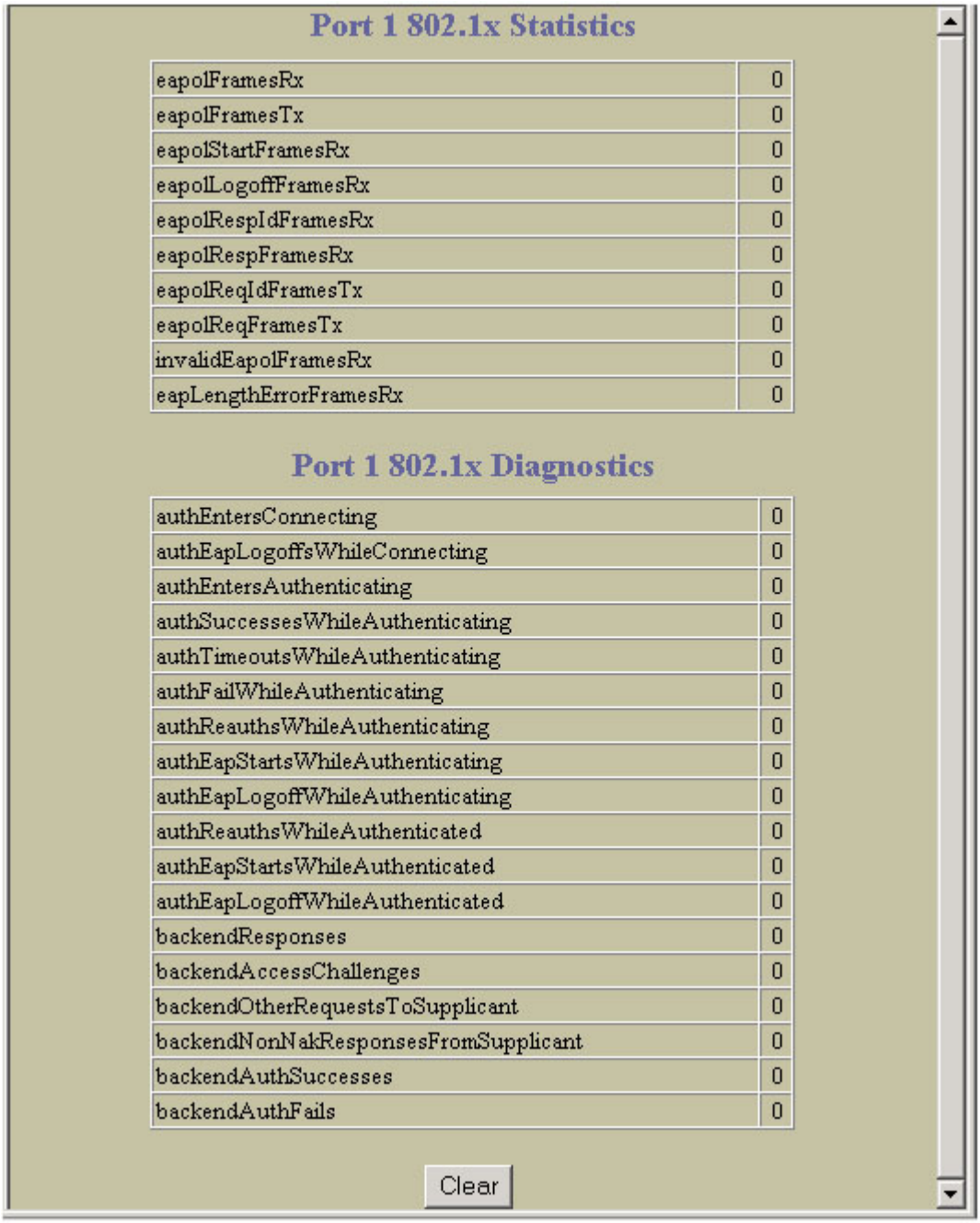
The following table describes 802.1x port statistics:

Table 61 Switch Port 802.1x Statistics

Statistic	Description
Port	Displays port numbers.
Last EAPOL Frame Source	Displays the MAC address of the most recent 802.1x frame received on the port.
Frame Version	Displays the version number of the most recent 802.1x frame received on the port.

Port 802.1x Statistics

To display the following form, go to the Switch Ports 802.1x Statistics form. Select a port number.



The following table describes 802.1x port statistics:

Table 62 Switch Port 802.1x Statistics

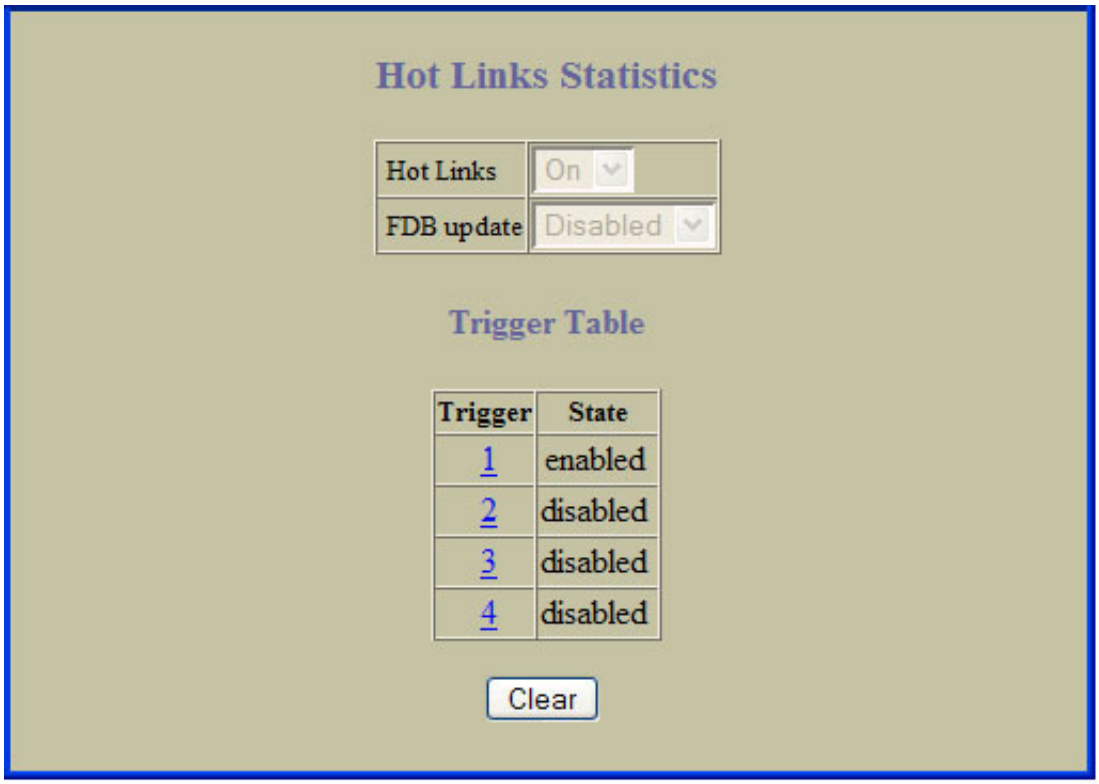
Statistic	Description
Authenticator Diagnostics	
`authEntersConnecting`	Total number of times that the state machine transitions to the CONNECTING state from any other state.
`authEapLogoffsWhileConnecting`	Total number of times that the state machine transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPOL-Logoff message.
`authEntersAuthenticating`	Total number of times that the state machine transitions from CONNECTING to AUTHENTICATING, as a result of an EAPResponse/ Identity message being received from the Supplicant.

Table 62 Switch Port 802.1x Statistics

Statistic	Description
authSuccessesWhile Authenticating	Total number of times that the state machine transitions from AUTHENTICATING to AUTHENTICATED, as a result of the Backend Authentication state machine indicating successful authentication of the Supplicant.
authTimeoutsWhileAuthenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of the Backend Authentication state machine indicating authentication timeout.
authFailWhileAuthenticating	Total number of times that the state machine transitions from AUTHENTICATING to HELD, as a result of the Backend Authentication state machine indicating authentication failure.
authReauthsWhileAuthenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of a re-authentication request
authEapStartsWhileAuthenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Start message being received from the Supplicant.
authEapLogoffWhileAuthenticating	Total number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Logoff message being received from the Supplicant.
authReauthsWhileAuthenticated	Total number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of a re-authentication request.
authEapStartsWhileAuthenticated	Total number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of an EAPOL-Start message being received from the Supplicant.
authEapLogoffWhileAuthenticated	Total number of times that the state machine transitions from AUTHENTICATED to DISCONNECTED, as a result of an EAPOLLogoff message being received from the Supplicant.
backendResponses	Total number of times that the state machine sends an initial Access-Request packet to the Authentication server. Indicates that the Authenticator attempted communication with the Authentication Server.
backendAccessChallenges	Total number of times that the state machine receives an initial Access-Challenge packet from the Authentication server. Indicates that the Authentication Server has communication with the Authenticator.
backendOtherRequestsToSupplicant	Total number of times that the state machine sends an EAP-Request packet (other than an Identity, Notification, Failure, or Success message) to the Supplicant. Indicates that the Authenticator chose an EAP-method.
backendNonNakResponsesFrom Supplicant	Total number of times that the state machine receives a response from the Supplicant to an initial EAP-Request, and the response is something other than EAP-NAK. Indicates that the Supplicant can respond to the Authenticators chosen EAP-method.
backendAuthSuccesses	Total number of times that the state machine receives an Accept message from the Authentication Server. Indicates that the Supplicant has successfully authenticated to the Authentication Server.
backendAuthFails	Total number of times that the state machine receives a Reject message from the Authentication Server. Indicates that the Supplicant has not authenticated to the Authentication Server.

Hot Links Statistics

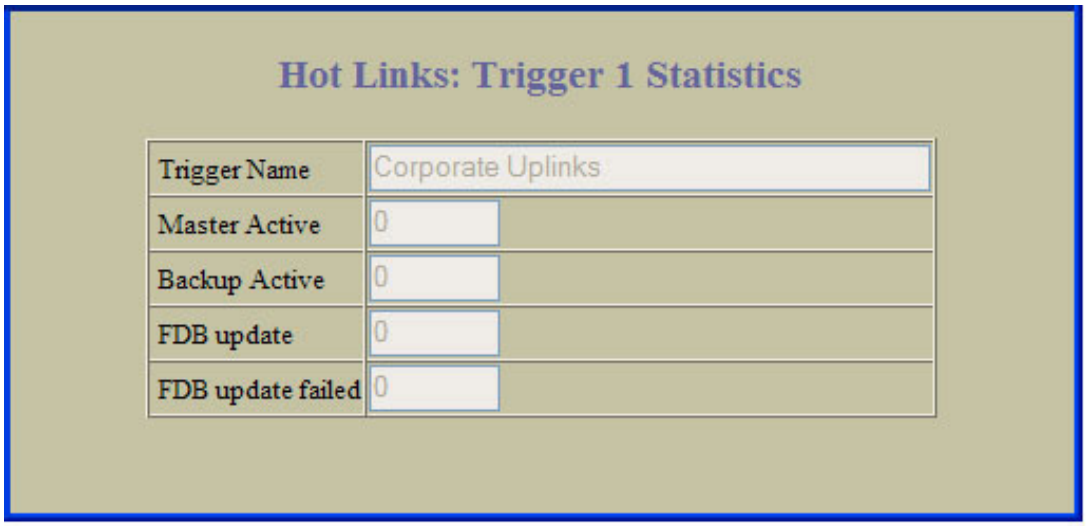
To display the following form, select **Layer 2 > Hot Links**.



Select a Trigger number to view statistics for the Trigger.

Hot Links Trigger Statistics

To display the following form, go to the Hot Links Statistics form, and select a Trigger number.



The following table describes Hot Links Trigger statistics:

Table 63 Hot Links Statistics

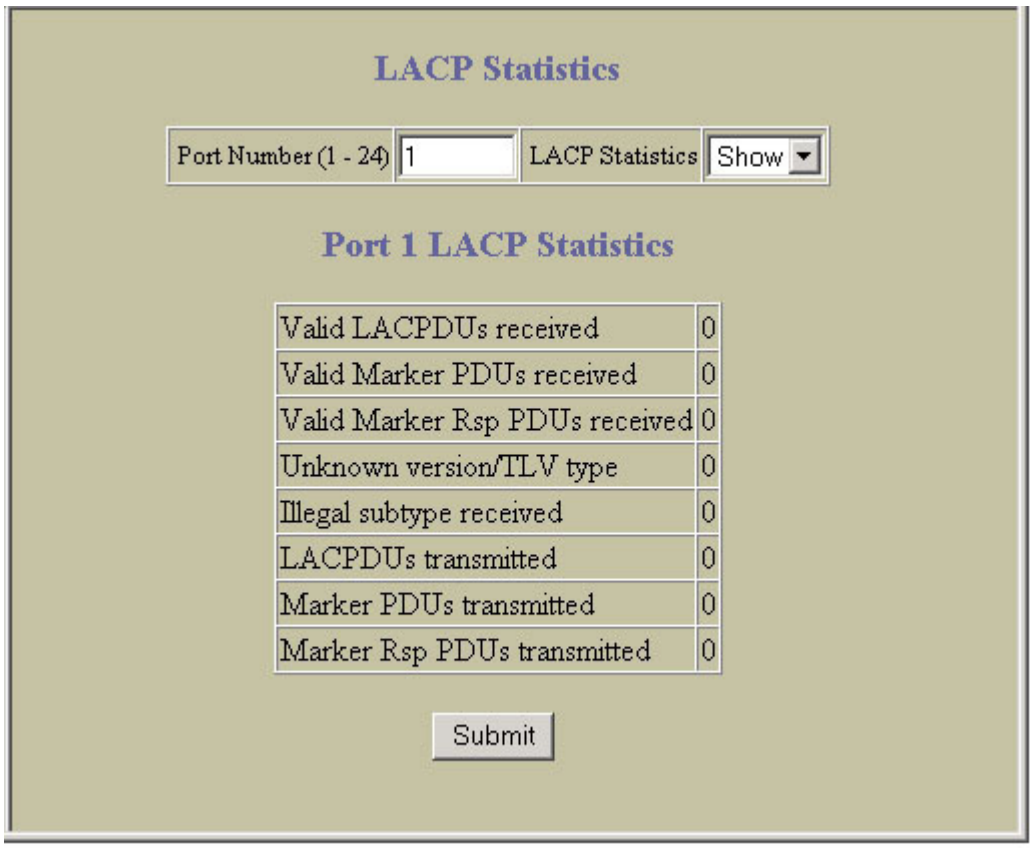
Statistic	Description
`Master active`	Total number of times the Master interface transitioned to the Active state.
`Backup active`	Total number of times the Backup interface transitioned to the Active state.
`FDB update`	Total number of FDB update requests sent.

Table 63 Hot Links Statistics

Statistic	Description
`failed`	Total number of FDB update requests that failed.

LACP Statistics

To display the following form, select **Layer 2 > LACP**.



Enter a port number to show LACP Statistics for the port. The following table describes LACP statistics:

Table 64 LACP Statistics

Statistic	Description
Port	Displays the port number.
Show	Enter a port number and select **Show** to display LACP statistics for the port.
Valid LACPDUs received	Total number of LACP data units received.
Valid Marker PDUs received	Not applicable (see note).
Valid Marker Rsp PDUs received	Not applicable (see note).
Unknown version/TLV type	Total number of LACPDUs received with an unknown version or TLV type.
Illegal subtype received	Total number LACPDUs received with an illegal subtype.
LACPDUs transmitted	Total number of LACP data units transmitted.
Marker PDUs transmitted	Not applicable (see note).
Marker Rsp PDUs transmitted	Not applicable (see note).

NOTE: Currently, LACP implementation does not support the Churn machine, an option used to detect if the port is operable within a bounded time period between the actor and the partner. Only the Marker Responder is implemented, and there is no marker protocol generator.

FDB Statistics

To display the following form, select **Layer 2 > FDB**.

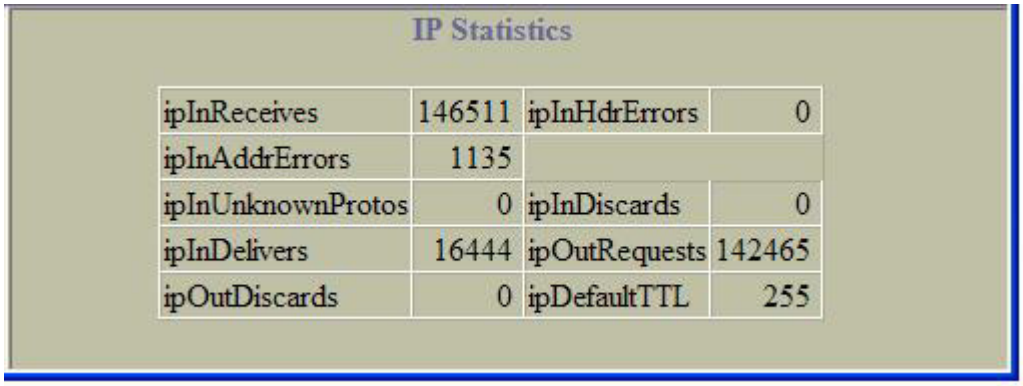
FDB statistics are described in the following table:

Table 65 Forwarding Database Statistics

Statistic	Description
Clear FDB Statistics	Select **Clear** and click **Submit** to clear FDB statistics.
current	Current number of entries in the Forwarding Database.
hiwat	Highest number of entries recorded at any given time in the Forwarding Database.

IP Statistics

To display the following form, select **Layer 3 > IP Interfaces** (click the underlined text, not the folder).



The following table describes IP statistics:

Table 66 IP Statistics

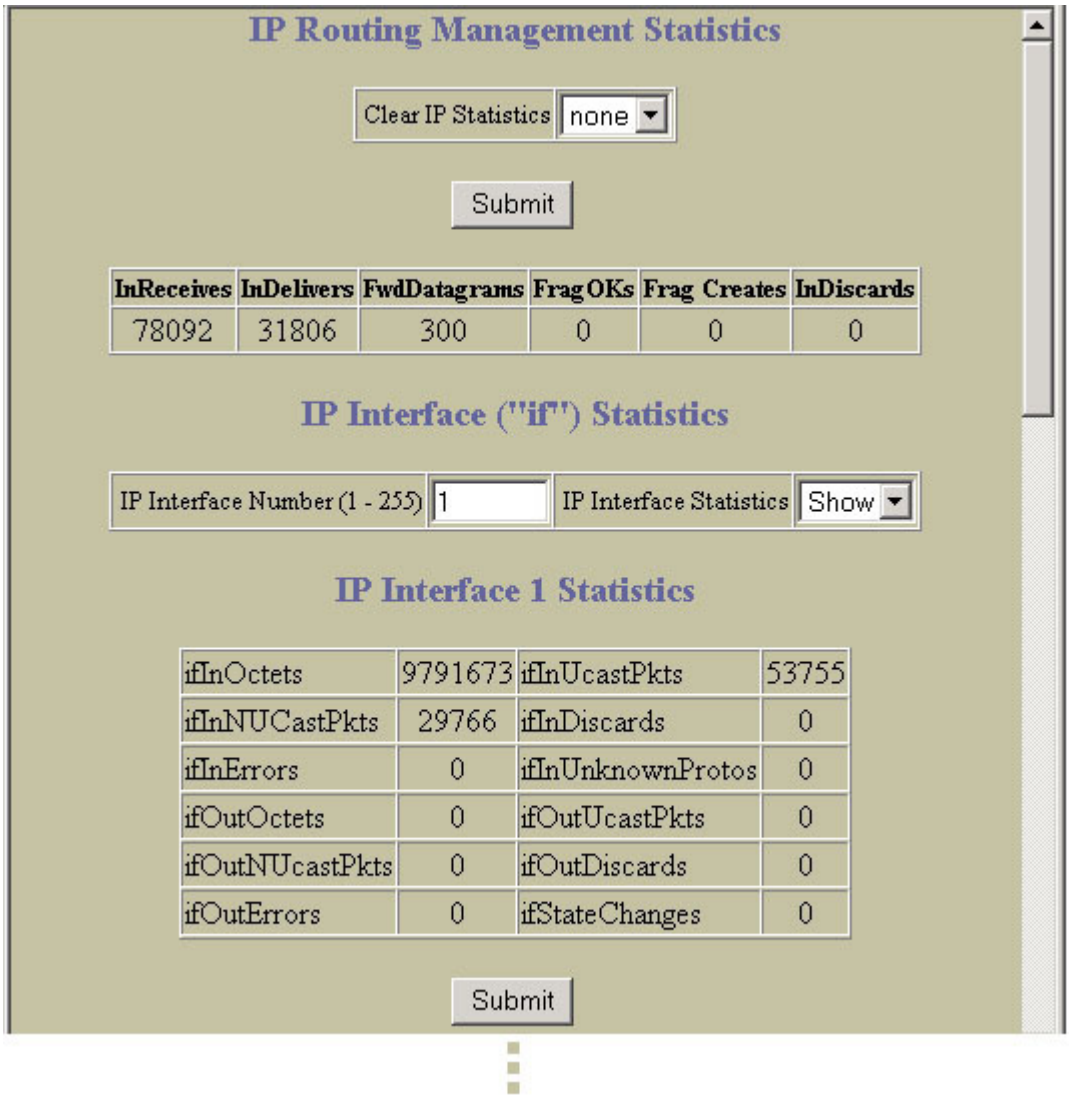
Statistic	Description
ipInReceives	The total number of input datagrams received from interfaces, including those received in error.
ipInAddrErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity (the switch). This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.

Table 66 IP Statistics

Statistic	Description
ipInUnknownProtos	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
ipInDelivers	The total number of input datagrams successfully delivered to IP userprotocols (including ICMP).
ipOutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space). Note that this counter would include datagrams counted in `ipForwDatagrams` if any such packets met this (discretionary) discard criterion.
ipInHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad `checksums`, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so forth.
ipInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
ipOutRequests	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in `ipForwDatagrams`.
ipDefaultTTL	The default value inserted into the Time-To-Live (TTL) field of the IP header of datagrams originated at this entity (the switch), whenever a TTL value is not supplied by the transport layer protocol.

IP Routing Management Statistics (part 1)

To display the following form, select **Layer 3 > Network Routes** (click the underlined text, not the folder).



The following table describes IP Routing Management statistics:

Table 67 IP Routing Management Statistics

Statistic	Description
InReceives	The total number of input datagrams received from interfaces, including those received in error.
InDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
FwdDatagrams	The number of input datagrams for which this entity (the switch) was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets, which were Source-Routed via this entity (the switch), and the Source- Route option processing was successful.
FragOKs	The number of IP datagrams that have been successfully fragmented at this entity (the switch).
FragCreates	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity (the switch).

Table 67 IP Routing Management Statistics

Statistic	Description
InDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). This counter does not include any datagrams discarded while awaiting re-assembly.

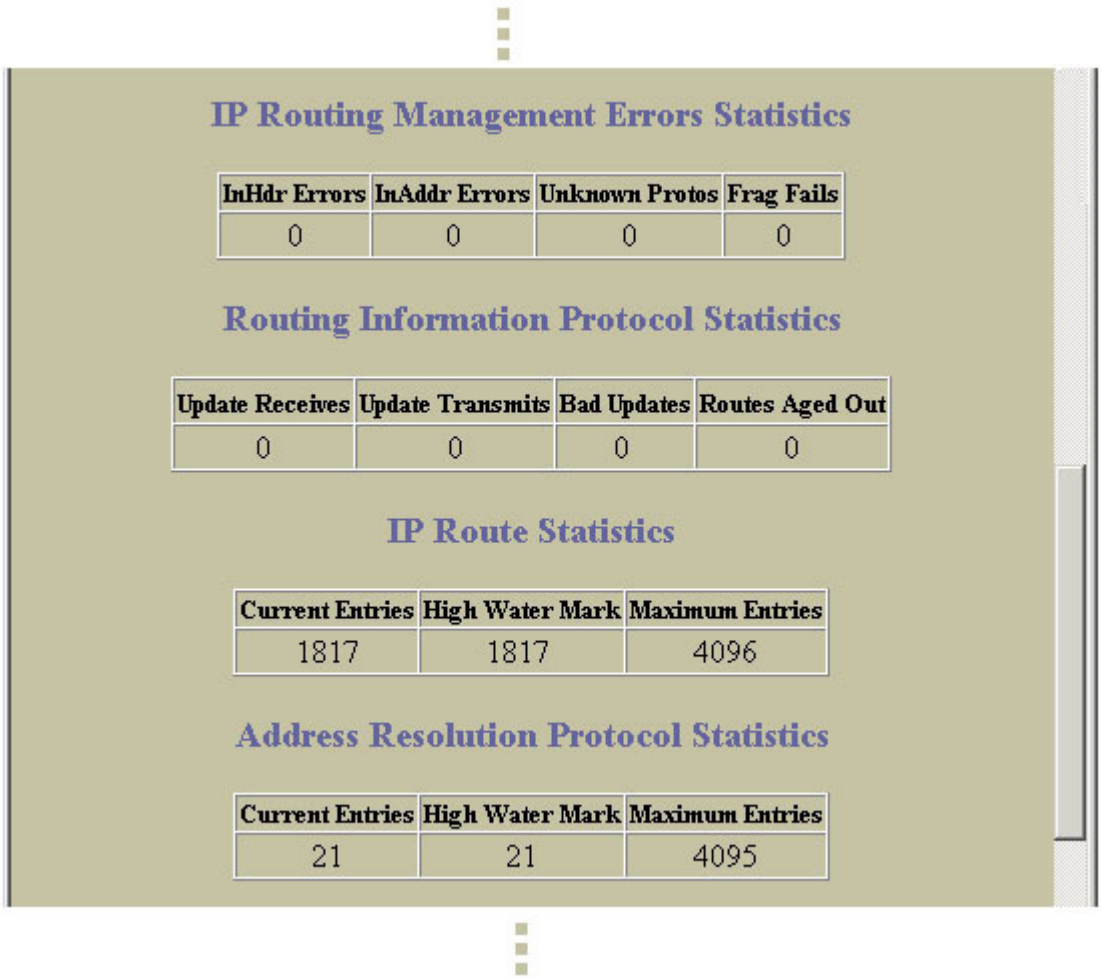
The following table describes the interface statistics:

Table 68 IF statistics

Statistics	Description
ifInOctets	The total number of octets received on the interface, including framing characters.
ifInUcastPkts	The number of packets, delivered by this sublayer to a higher sublayer, which were not addressed to a multicast or broadcast address at this sublayer.
ifInNUCastPkts	The number of packets, delivered by this sublayer to a higher sublayer, which were addressed to a multicast or broadcast address at this sublayer. This object is deprecated in favor of `ifInMulticastPkts` and `ifInBroadcastPkts`.
ifInDiscards	The number of inbound packets that were chosen to be discarded even though no errors were detected to prevent their being delivered to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
ifInErrors	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.
ifInUnknownProtos	For packet-oriented interfaces, the number of packets received via the interfaces that were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces which support protocol multiplexing the number of transmission units received via the interface which were discarded because of an unknown or unsupported protocol. For any interface that does not support protocol multiplexing, this counter will always be zero (0).
ifOutOctets	The total number of octets transmitted out of the interface, including framing characters.
ifOutUcastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were not addressed to a multicast or broadcast address at this sublayer, including those that were discarded or not sent.
ifOutNUcastPkts	The total number of packets that higher-level protocols requested to be transmitted, and which were addressed to a multicast or broadcast address at this sublayer, including those that were discarded or not sent. This object is deprecated in favor of `ifOutMulticastPkts` and `ifOutBroadcastPkts`.
ifOutDiscards	The number of outbound packets, which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
ifOutErrors	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.
ifStateChanges	The number of times an interface has transitioned from either down to up or from up to down.

IP Routing Management Statistics (part 2)

To display the following form, select **Layer 3 > Network Routes** (click the underlined text, not the folder).



The following table describes IP Routing Management statistics:

Table 69 IP Routing Management Statistics

Statistic	Description
`InHdrErrors`	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so on.
`InAddrErrors`	The number of input datagrams discarded because the IP address in their IP header destination field was not a valid address to be received at this GbE2 Interconnect Switch. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported classes (for example, Class E). For entities which are not IP gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
`UnknownProtos`	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
`FragFails`	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity (the switch) but could not be, for example, because their `Don't Fragment` flag was set.

The following table describes Routing Information Protocol statistics:

Table 70 Routing Information Protocol Statistics

Statistic	Description
Update Receives	The total number of good RIP advertisement packets received.
Update Transmits	The total number of RIP advertisement packets sent.
Bad Updates	The total number of RIP advertisement packets received that were dropped.
Routes Aged Out	The total number of routes learned via RIP that has aged out.

The following table describes the IP Route statistics:

Table 71 Route statistics

Statistics	Description
Current Entries	The total number of outstanding routes in the route table.
High Water Mark	The highest number of routes ever recorded in the route table.
Maximum Entries	The maximum number of supported routes.

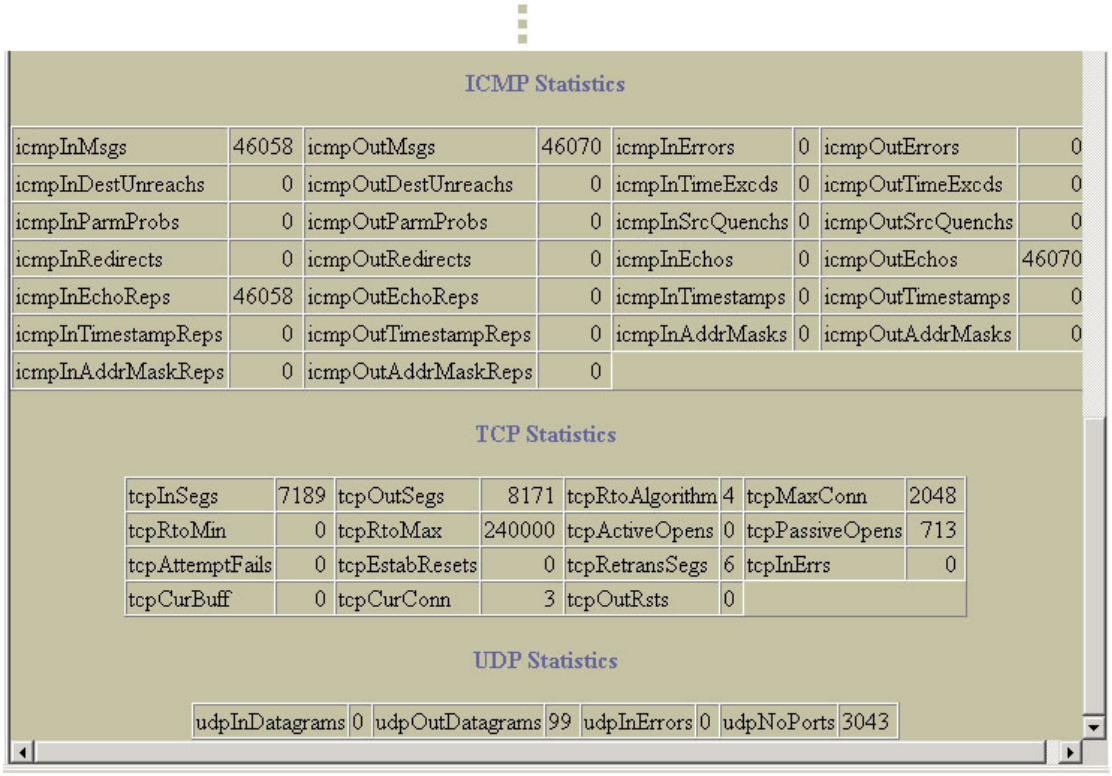
The following table describes the Address Resolution Protocol (ARP) statistics:

Table 72 ARP statistics

Statistic	Description
Current Entries	The total number of outstanding ARP entries in the ARP table.
High Water Mark	The highest number of ARP entries ever recorded in the ARP table.
Maximum Entries	Total number of ARP entries allowed in the ARP table.

IP Routing Management Statistics (part 3)

To display the following form, select **Layer 3 > Network Routes** (click the underlined text, not the folder).



ICMP Statistics

icmpInMsgs	46058	icmpOutMsgs	46070	icmpInErrors	0	icmpOutErrors	0
icmpInDestUnreachs	0	icmpOutDestUnreachs	0	icmpInTimeExcds	0	icmpOutTimeExcds	0
icmpInParmProbs	0	icmpOutParmProbs	0	icmpInSrcQuenchs	0	icmpOutSrcQuenchs	0
icmpInRedirects	0	icmpOutRedirects	0	icmpInEchos	0	icmpOutEchos	46070
icmpInEchoReps	46058	icmpOutEchoReps	0	icmpInTimestamps	0	icmpOutTimestamps	0
icmpInTimestampReps	0	icmpOutTimestampReps	0	icmpInAddrMasks	0	icmpOutAddrMasks	0
icmpInAddrMaskReps	0	icmpOutAddrMaskReps	0				

TCP Statistics

tcpInSegs	7189	tcpOutSegs	8171	tcpRtoAlgorithm	4	tcpMaxConn	2048
tcpRtoMin	0	tcpRtoMax	240000	tcpActiveOpens	0	tcpPassiveOpens	713
tcpAttemptFails	0	tcpEstabResets	0	tcpRetransSegs	6	tcpInErrs	0
tcpCurBuff	0	tcpCurConn	3	tcpOutRsts	0		

UDP Statistics

udpInDatagrams	0	udpOutDatagrams	99	udpInErrors	0	udpNoPorts	3043

The following table describes the Internet Control Messaging Protocol (ICMP) statistics:

Table 73 ICMP statistics

Statistics	Description
icmpInMsgs	The total number of ICMP messages which the GbE2 Interconnect Switch received. Note that this counter includes all those counted by **icmpInErrors**.
icmpInErrors	The number of ICMP messages which the GbE2 Interconnect Switch received but determined as having ICMP specific errors (for example bad ICMP checksums and bad length).
icmpInDestUnreachs	The number of ICMP **Destination Unreachable** messages received.
icmpInTimeExcds	The number of ICMP **Time Exceeded** messages received.
icmpInParmProbs	The number of ICMP **Parameter Problem** messages received.
icmpInSrcQuenchs	The number of ICMP **Source Quench** (buffer almost full, stop sending data) messages received.
icmpInRedirects	The number of ICMP **Redirect** messages received.
icmpInEchos	The number of ICMP **Echo** (request) messages received.
icmpInEchoReps	The number of ICMP **Echo Reply** messages received.
icmpInTimestamps	The number of ICMP **Timestamp** (request) messages received.
icmpInTimestampReps	The number of ICMP **Timestamp Reply** messages received.
icmpInAddrMasks	The number of ICMP **Address Mask Request** messages received.
icmpInAddrMaskReps	The number of ICMP **Address Mask Reply** messages received.
icmpOutMsgs	The total number of ICMP messages which this GbE2 Interconnect Switch attempted to send. Note that this counter includes all those counted by **icmpOutErrors.**
icmpOutErrors	The number of ICMP messages that this GbE2 Interconnect Switch did not send due to problems discovered within ICMP such as a lack of buffer. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of errors that contribute to this counter's value.
icmpOutDestUnreachs	The number of ICMP **Destination Unreachable** messages sent.
icmpOutTimeExcds	The number of ICMP **Time Exceeded** messages sent.
icmpOutParmProbs	The number of ICMP **Parameter Problem** messages sent.
icmpOutSrcQuenchs	The number of ICMP **Source Quench** (buffer almost full, stop sending data) messages sent.
icmpOutRedirects	The number of ICMP **Redirect** messages sent.
icmpOutEchos	The number of ICMP **Echo** (request) messages sent.
icmpOutEchoReps	The number of ICMP **Echo Reply** messages sent.
icmpOutTimestamps	The number of ICMP **Timestamp** (request) messages sent.
icmpOutTimestampReps	The number of ICMP **Timestamp Reply** messages sent.
icmpOutAddrMasks	The number of ICMP **Address Mask Request** messages sent.
icmpOutAddrMaskReps	The number of ICMP **Address Mask Reply** messages sent.

The following table describes the Transmission Control Protocol (TCP) statistics:

Table 74 TCP statistics

Statistics	Description
tcpRtoAlgorithm	The algorithm used to determine the timeout value used for retransmitting unacknowledged octets.
tcpRtoMin	The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the LBOUND quantity described in Request For Comments (RFC) 793.
tcpRtoMax	The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the UBOUND quantity described in RFC 793.
tcpMaxConn	The limit on the total number of TCP connections the GbE2 Interconnect Switch can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.
tcpActiveOpens	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
tcpPassiveOpens	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
tcpAttemptFails	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
tcpEstabResets	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE- WAIT state.
tcpInSegs	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
tcpOutSegs	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
tcpRetransSegs	The total number of segments retransmitted, that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
tcpInErrs	The total number of segments received in error (for example, bad TCP checksums).
tcpCurBuff	The total number of outstanding memory allocations from heap by TCP protocol stack.
tcpCurConn	The total number of outstanding TCP sessions that are currently opened.
tcpOutRsts	The number of TCP segments sent containing the reset (RST) flag.

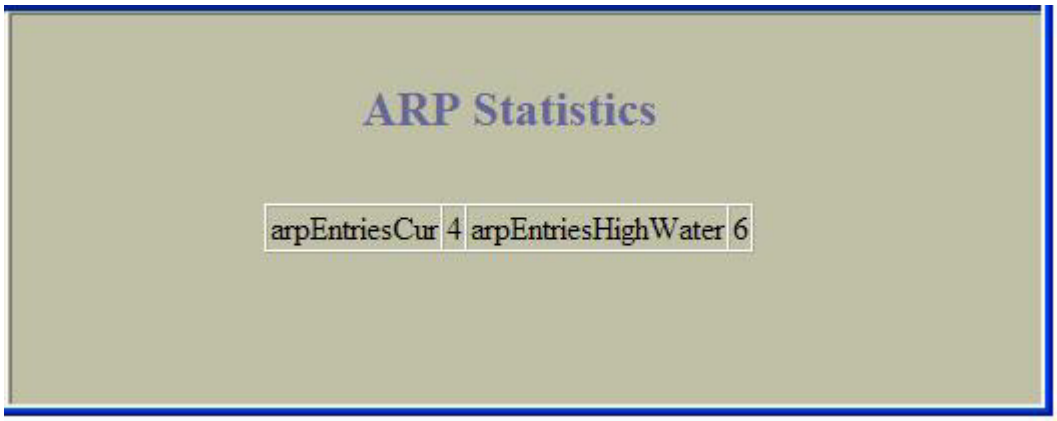
The following table describes the User Datagram Protocol (UDP) statistics:

Table 75 UDP statistics

Statistics	Description
udpInDatagrams	The total number of UDP datagrams delivered to the GbE2 Interconnect Switch.
udpOutDatagrams	The total number of UDP datagrams sent from this GbE2 Interconnect Switch.
udpInErrors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
udpNoPorts	The total number of received UDP datagrams for which there was no application at the destination port.

ARP Statistics

To display the following form, select **Layer 3 > ARP** (click the underlined text, not the folder).



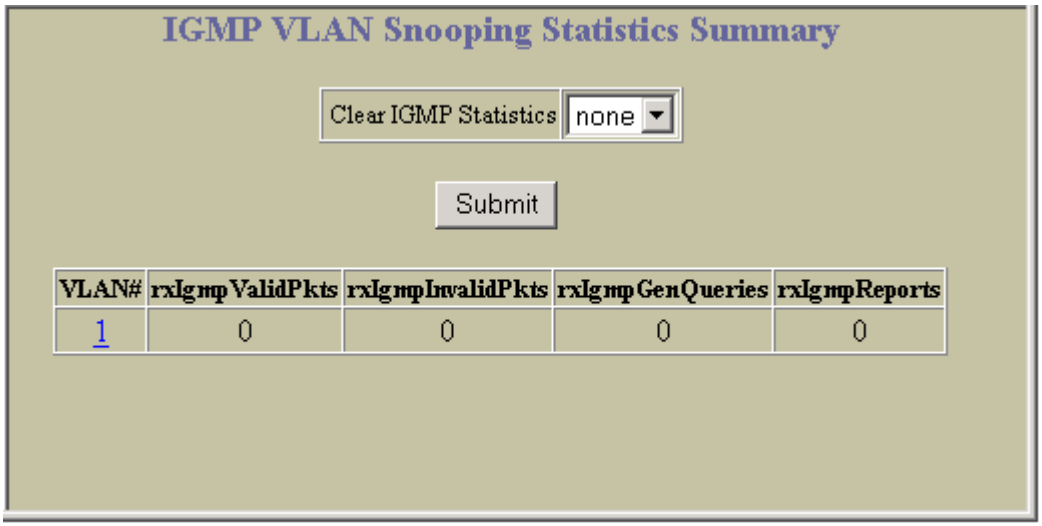
The following table describes Address Resolution Protocol (ARP) statistics:

Table 76 ARP Statistics

Statistic	Description
arpEntriesCur	The total number of outstanding ARP entries in the ARP table.
arpEntriesHighWater	The highest number of ARP entries ever recorded in the ARP table.

IGMP VLAN Snooping Statistics Summary

To display the following form, select **Layer 3 > IGMP > IGMP Snooping** (click the underlined text, not the folder).



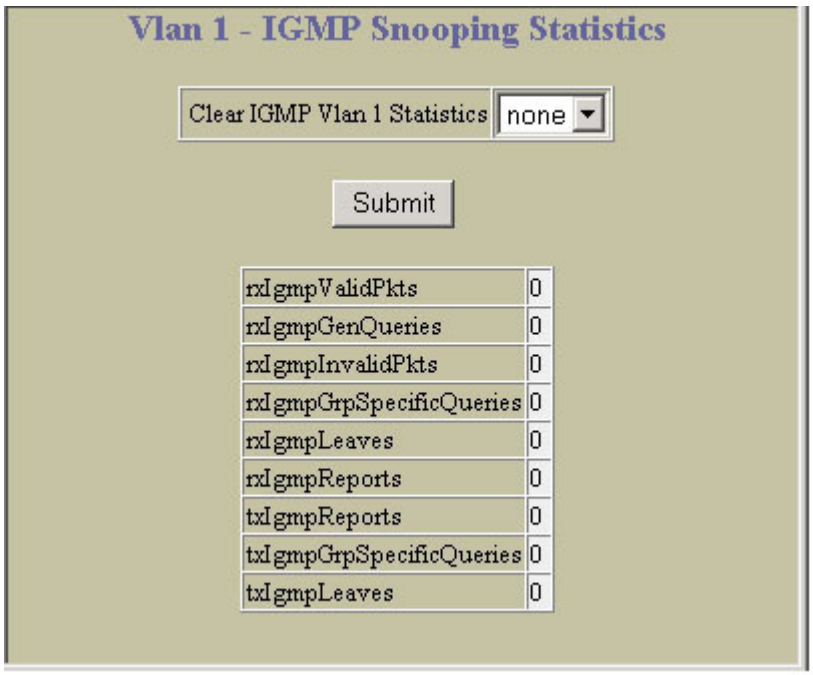
The following table describes IGMP VLAN snooping statistics:

Table 77 IGMP VLAN Snooping Statistics Summary

Statistic	Description
Clear IGMP Statistics	Select **Clear** and click **Submit** to clear all IGMP statistics.
VLAN#	Selects a VLAN.
rxIgmpValidPkts	The total number of valid IGMP packets received.
rxIgmpInvalidPkts	The total number of invalid packets received.
rxIgmpGenQueries	The total number of General Membership Query packets received.
rxIgmpReports	The total number of Membership Reports received.

VLAN - IGMP Snooping Statistics

To display the following form, go to the IGMP VLAN Snooping Statistics Summary form. Select a VLAN number.



The following table describes IGMP VLAN snooping statistics for the selected VLAN:

Table 78 VLAN - Snooping Statistics Summary

Statistic	Description
Clear IGMP VLAN x Statistics	Select **Clear** and click **Submit** to clear IGMP statistics for this VLAN.
rxIgmpValidPkts	Total number of valid IGMP packets received
rxIgmpGenQueries	Total number of General Membership Query packets received
rxIgmpInvalidPkts	Total number of invalid packets received
rxIgmpGrpSpecificQueries	Total number of Membership Query packets received from specific groups
rxIgmpLeaves	Total number of Leave requests received
rxIgmpReports	Total number of Membership Reports received
txIgmpReports	Total number of Membership reports transmitted
txIgmpGrpSpecificQueries	Total number of Membership Query packets transmitted to specific groups
txIgmpLeaves	Total number of Leave message transmitted

OSPF General Statistics

To display the following form, select **Layer 3 > OSPF > General**.

OSPF General Statistics

OSPF Rx/Tx Statistics

	Rx Statistics		Tx Statistics
Pkts	12589	Pkts	14152
hello	9358	hello	9249
database	28	database	27
ls requests	1	ls requests	200
ls acks	248	ls acks	4427
ls updates	2954	ls updates	248

OSPF Neighbor Change Statistics

	Nbr Statistics		Nbr Statistics
hello	1	bad requests	0
start	0	bad sequence	0
n2way	1	loading done	1
adjoint ok	1	n1way	0
negotiation done	1	rst_ad	0
exchange done	1	down	0

OSPF Interface Change Statistics

	Intf Statistics
up	1
down	0
loop	0
unloop	0
wait timer	0
backup	1
nbr change	0

OSPF Timer KickOff Statistics

	Timer kickoff
hello	9252
retransmit	18505
lsa lock	18512
lsa ack	92565
dbage	46282
summary	30854
ase export	46272

The following table describes OSPF General statistics:

Table 79 OSPF General Statistics

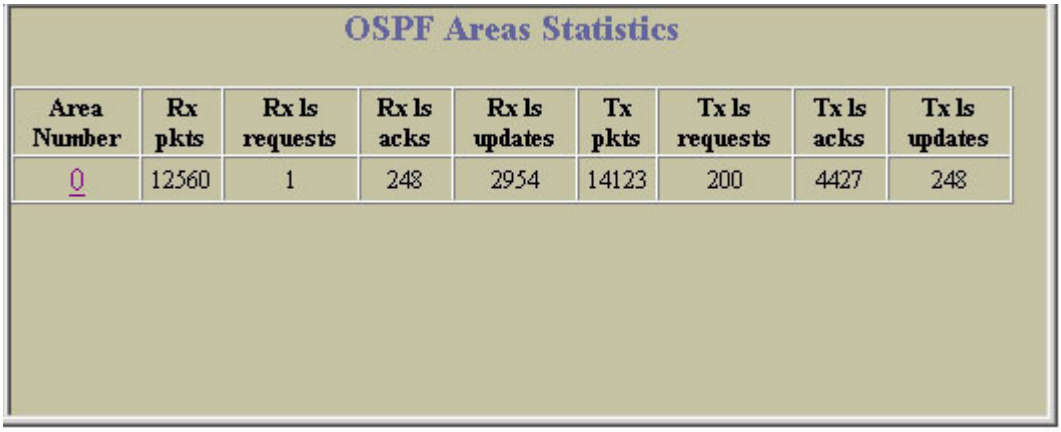
Statistic	Description
OSPF Rx/Tx Statistics	
Rx Statistics	
`pkts`	The sum total of all OSPF packets received on all OSPF areas and interfaces.
`hello`	The sum total of all Hello packets received on all OSPF areas and interfaces.
`database`	The sum total of all Database Description packets received on all OSPF areas and interfaces.
`ls requests`	The sum total of all Link State Request packets received on all OSPF areas and interfaces.
`ls acks`	The sum total of all Link State Acknowledgement packets received on all OSPF areas and interfaces.
`ls updates`	The sum total of all Link State Update packets received on all OSPF areas and interfaces.
Tx Statistics	
`pkts`	The sum total of all OSPF packets transmitted on all OSPF areas and interfaces.
`hello`	The sum total of all Hello packets transmitted on all OSPF areas and interfaces.
`database`	The sum total of all Database Description packets transmitted on all OSPF areas and interfaces.
`ls requests`	The sum total of all Link State Request packets transmitted on all OSPF areas and interfaces.
`ls acks`	The sum total of all Link State Acknowledgement packets transmitted on all OSPF areas and interfaces.
`ls updates`	The sum total of all Link State Update packets transmitted on all OSPF areas and interfaces.
OSPF Neighbor Change Statistics	
`hello`	The sum total of all Hello packets received from neighbors on all OSPF areas and interfaces.
`start`	The sum total number of neighbors in this state (that is, an indication that Hello packets should now be sent to the neighbor at intervals of `HelloInterval` seconds) across all OSPF areas and interfaces.
`n2way`	The sum total number of bidirectional communication establishment between this router and other neighboring routers.
`adjoint ok`	The sum total number of decisions to be made (again) as to whether an adjacency should be established/maintained with the neighbor across all OSPF areas and interfaces.
`negotiation done`	The sum total number of neighbors in this state wherein the Master/slave relationship has been negotiated, and sequence numbers have been exchanged, across all OSPF areas and interfaces.
`exchange done`	The sum total number of neighbors in this state (that is, in an adjacency's final state) having transmitted a full sequence of Database Description packets, across all OSPF areas and interfaces.
`bad requests`	The sum total number of Link State Requests which have been received for a link state advertisement not contained in the database across all interfaces and OSPF areas.

Table 79 OSPF General Statistics

Statistic	Description
bad sequence	The sum total number of Database Description packets which have been received that either: a) Has an unexpected DD sequence number b) Unexpectedly has the init bit set c) Has an options field differing from the last Options field received in a Database Description packet. Any of these conditions indicate that some error has occurred during adjacency establishment for all OSPF areas and interfaces.
loading done	The sum total number of link state updates received for all out-of-date portions of the database across all OSPF areas and interfaces.
n1way	The sum total number of Hello packets received from neighbors, in which this router is not mentioned across all OSPF interfaces and areas.
rst_ad	The sum total number of times the Neighbor adjacency has been reset across all OPSF areas and interfaces.
down	The total number of Neighboring routers down (that is, in the initial state of a neighbor conversation) across all OSPF areas and interfaces.
OSPF Interface Change Statistics	
hello	The sum total number of Hello packets sent on all interfaces and areas.
down	The sum total number of interfaces down in all OSPF areas.
loop	The sum total of interfaces no longer connected to the attached network across all OSPF areas and interfaces.
unloop	The sum total number of interfaces, connected to the attached network in all OSPF areas.
wait timer	The sum total number of times the Wait Timer has been fired, indicating the end of the waiting period that is required before electing a (Backup) Designated Router across all OSPF areas and interfaces.
backup	The sum total number of Backup Designated Routers on the attached network for all OSPF areas and interfaces.
nbr change	The sum total number of changes in the set of bidirectional neighbors associated with any interface across all OSPF areas.

OSPF Areas Statistics

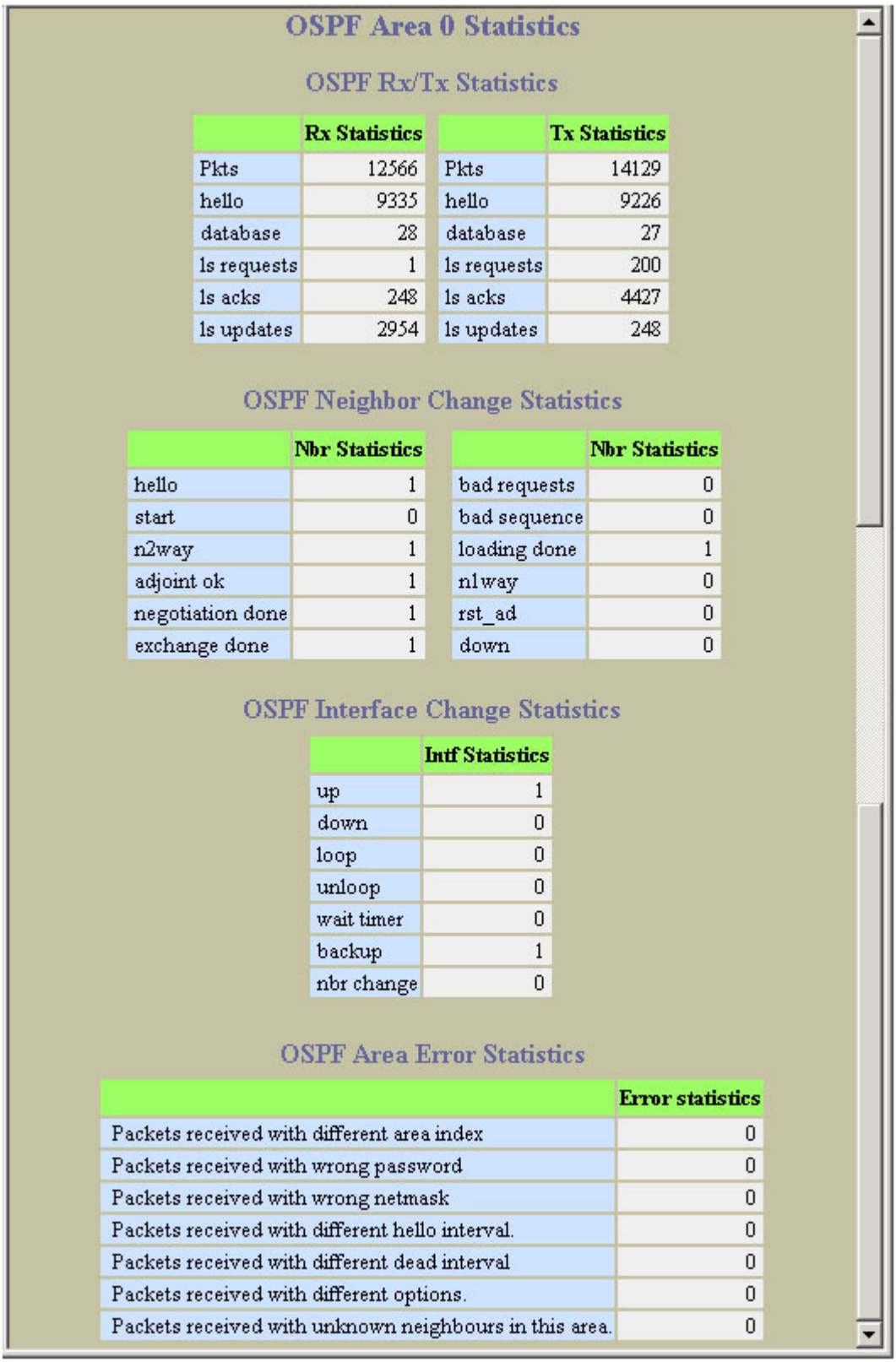
To display the following form, select **Layer 3 > OSPF > OSPF Areas** (click the underlined text, not the folder).



Select an area number to view detailed statistics.

OSPF Area Statistics

To display the following form, go to the OSPF Areas Statistics form. Select an area number.



OSPF Area 0 Statistics

OSPF Rx/Tx Statistics

	Rx Statistics		Tx Statistics
Pkts	12566	Pkts	14129
hello	9335	hello	9226
database	28	database	27
ls requests	1	ls requests	200
ls acks	248	ls acks	4427
ls updates	2954	ls updates	248

OSPF Neighbor Change Statistics

	Nbr Statistics		Nbr Statistics
hello	1	bad requests	0
start	0	bad sequence	0
n2way	1	loading done	1
adjoint ok	1	n1way	0
negotiation done	1	rst_ad	0
exchange done	1	down	0

OSPF Interface Change Statistics

	Intf Statistics
up	1
down	0
loop	0
unloop	0
wait timer	0
backup	1
nbr change	0

OSPF Area Error Statistics

	Error statistics
Packets received with different area index	0
Packets received with wrong password	0
Packets received with wrong netmask	0
Packets received with different hello interval.	0
Packets received with different dead interval	0
Packets received with different options.	0
Packets received with unknown neighbours in this area.	0

The following table describes OSPF Area statistics:

Table 80 OSPF Area Statistics

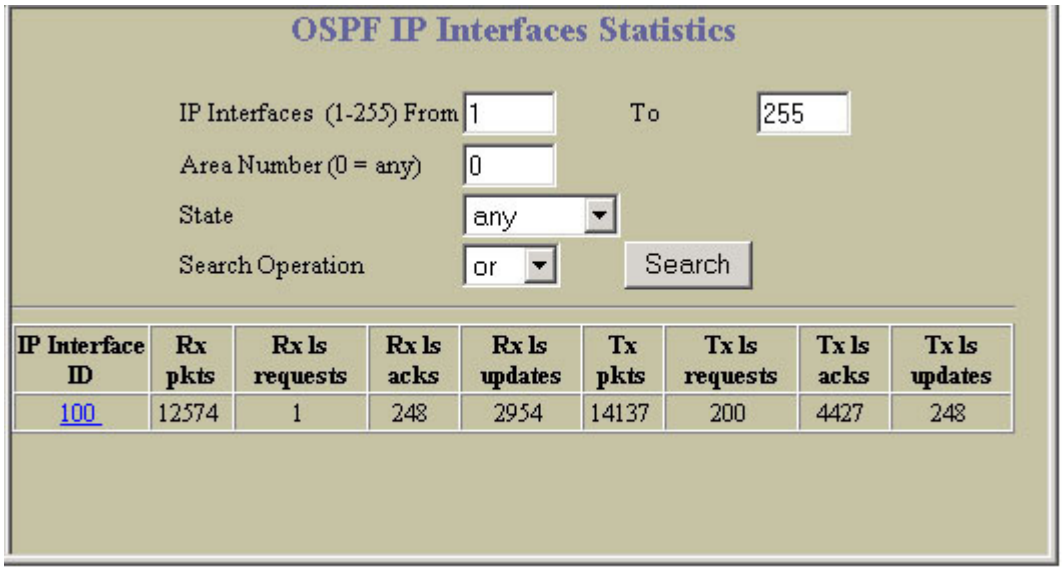
Statistic	Description
OSPF Rx/Tx Statistics	
Rx Statistics	
`pkts`	The sum total of all OSPF packets received on all OSPF areas and interfaces.
`hello`	The sum total of all Hello packets received on all OSPF areas and interfaces.
`database`	The sum total of all Database Description packets received on all OSPF areas and interfaces.
`ls requests`	The sum total of all Link State Request packets received on all OSPF areas and interfaces.
`ls acks`	The sum total of all Link State Acknowledgement packets received on all OSPF areas and interfaces.
`ls updates`	The sum total of all Link State Update packets received on all OSPF areas and interfaces.
Tx Statistics	
`pkts`	The sum total of all OSPF packets transmitted on all OSPF areas and interfaces.
`hello`	The sum total of all Hello packets transmitted on all OSPF areas and interfaces.
`database`	The sum total of all Database Description packets transmitted on all OSPF areas and interfaces.
`ls requests`	The sum total of all Link State Request packets transmitted on all OSPF areas and interfaces.
`ls acks`	The sum total of all Link State Acknowledgement packets transmitted on all OSPF areas and interfaces.
`ls updates`	The sum total of all Link State Update packets transmitted on all OSPF areas and interfaces.
OSPF Neighbor Change Statistics	
`hello`	The sum total of all Hello packets received from neighbors on all OSPF areas and interfaces.
`start`	The sum total number of neighbors in this state (that is, an indication that Hello packets should now be sent to the neighbor at intervals of `HelloInterval` seconds) across all OSPF areas and interfaces.
`n2way`	The sum total number of bidirectional communication establishment between this router and other neighboring routers.
`adjoint ok`	The sum total number of decisions to be made (again) as to whether an adjacency should be established/maintained with the neighbor across all OSPF areas and interfaces.
`negotiation done`	The sum total number of neighbors in this state wherein the Master/slave relationship has been negotiated, and sequence numbers have been exchanged, across all OSPF areas and interfaces.
`exchange done`	The sum total number of neighbors in this state (that is, in an adjacency's final state) having transmitted a full sequence of Database Description packets, across all OSPF areas and interfaces.
`bad requests`	The sum total number of Link State Requests which have been received for a link state advertisement not contained in the database across all interfaces and OSPF areas.

Table 80 OSPF Area Statistics

Statistic	Description
`bad sequence`	The sum total number of Database Description packets which have been received that either: a) Has an unexpected DD sequence number b) Unexpectedly has the init bit set c) Has an options field differing from the last Options field received in a Database Description packet. Any of these conditions indicate that some error has occurred during adjacency establishment for all OSPF areas and interfaces.
`loading done`	The sum total number of link state updates received for all out-of-date portions of the database across all OSPF areas and interfaces.
`n1way`	The sum total number of Hello packets received from neighbors, in which this router is not mentioned across all OSPF interfaces and areas.
`rst_ad`	The sum total number of times the Neighbor adjacency has been reset across all OPSF areas and interfaces.
`down`	The total number of Neighboring routers down (that is, in the initial state of a neighbor conversation) across all OSPF areas and interfaces.
OSPF Interface Change Statistics	
`hello`	The sum total number of Hello packets sent on all interfaces and areas.
`down`	The sum total number of interfaces down in all OSPF areas.
`loop`	The sum total of interfaces no longer connected to the attached network across all OSPF areas and interfaces.
`unloop`	The sum total number of interfaces, connected to the attached network in all OSPF areas.
`wait timer`	The sum total number of times the Wait Timer has been fired, indicating the end of the waiting period that is required before electing a (Backup) Designated Router across all OSPF areas and interfaces.
`backup`	The sum total number of Backup Designated Routers on the attached network for all OSPF areas and interfaces.
`nbr change`	The sum total number of changes in the set of bidirectional neighbors associated with any interface across all OSPF areas.

OSPF IP Interfaces Statistics

To display the following form, select **Layer 3 > OSPF > OSPF Interfaces** (click the underlined text, not the folder).



The following table describes the OSPF IP Interfaces Statistics controls:

Table 81 OSPF IP Interface statistics

Control	Description
Search Operation	To focus the search for an OSPF IP interface, enter search parameters: • IP Interfaces • Area number • State Fields that have a value of "any" are ignored during the search. Choose a search operation: • **or**: Search for OSPF IP interfaces specified in the Search range that meet any of the criteria entered. • **and**: Search for OSPF IP interfaces specified in the Search range that meet all of the criteria entered. Click **Search** to display OSPF IP interfaces that fit the range and meet the criteria entered.

Select an interface ID number to view detailed statistics.

OSPF IP Interface Statistics

To display the following form, go to the OSPF IP Interfaces Statistics form. Select an interface ID number.

OSPF Interface 100 Statistics

OSPF Rx/Tx Statistics

	Rx Statistics		Tx Statistics
Pkts	12580	Pkts	14142
hello	9349	hello	9239
database	28	database	27
ls requests	1	ls requests	200
ls acks	248	ls acks	4427
ls updates	2954	ls updates	248

OSPF Neighbor Change Statistics

	Nbr Statistics		Nbr Statistics
hello	1	bad requests	0
start	0	bad sequence	0
n2way	1	loading done	1
adjoint ok	1	n1way	0
negotiation done	1	rst_ad	0
exchange done	1	down	0

OSPF Interface Change Statistics

	Intf Statistics
up	1
down	0
loop	0
unloop	0
wait timer	0
backup	1
nbr change	0

OSPF Interface Error Statistics

	Error Statistics
Packets received with different area index	0
Packets received with wrong password	0
Packets received with wrong netmask	0
Packets received with different hello interval.	0
Packets received with different dead interval	0
Packets received with different options.	0
Packets received with unknown neighbours in this area.	0

The following table describes OSPF interface statistics:

Table 82 OSPF Interface Statistics

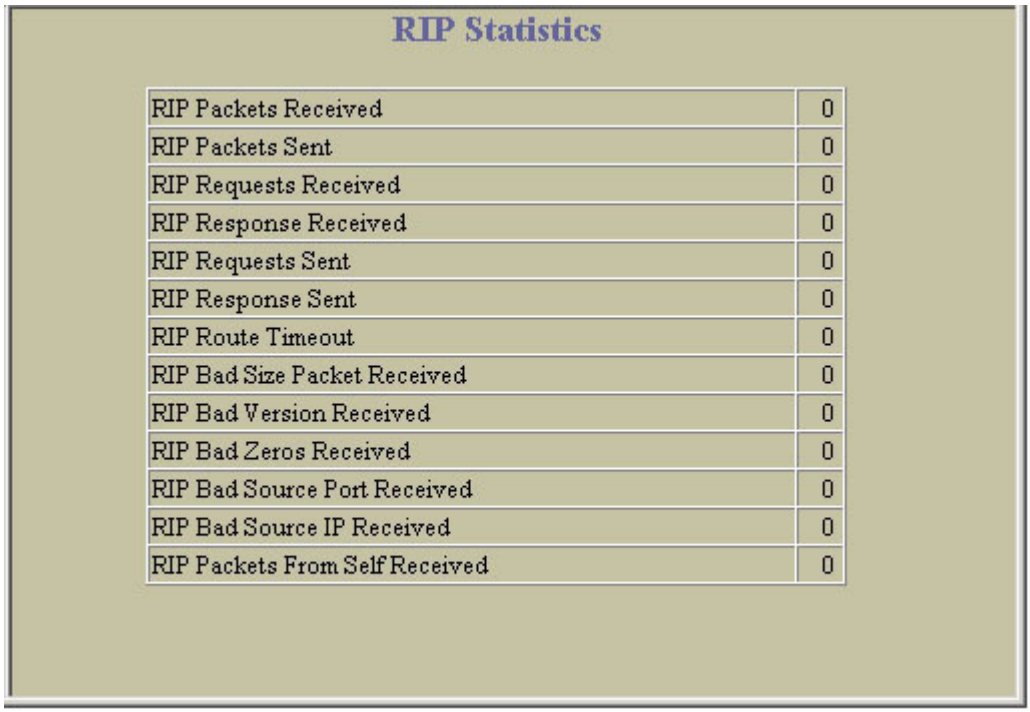
Statistic	Description
OSPF Rx/Tx Statistics	
Rx Statistics	
`Pkts`	The sum total of all OSPF packets received on all OSPF areas and interfaces.
`hello`	The sum total of all Hello packets received on all OSPF areas and interfaces.
`database`	The sum total of all Database Description packets received on all OSPF areas and interfaces.
`ls Requests`	The sum total of all Link State Request packets received on all OSPF areas and interfaces.
`ls Acks`	The sum total of all Link State Acknowledgement packets received on all OSPF areas and interfaces.
`ls Updates`	The sum total of all Link State Update packets received on all OSPF areas and interfaces.
Tx Statistics	
`pkts`	The sum total of all OSPF packets transmitted on all OSPF areas and interfaces.
`hello`	The sum total of all Hello packets transmitted on all OSPF areas and interfaces.
`database`	The sum total of all Database Description packets transmitted on all OSPF areas and interfaces.
`ls Requests`	The sum total of all Link State Request packets transmitted on all OSPF areas and interfaces.
`ls Acks`	The sum total of all Link State Acknowledgement packets transmitted on all OSPF areas and interfaces.
`ls Updates`	The sum total of all Link State Update packets transmitted on all OSPF areas and interfaces.
OSPF Neighbor Change Statistics	
`hello`	The sum total of all Hello packets received from neighbors on all OSPF areas and interfaces.
`start`	The sum total number of neighbors in this state (that is, an indication that Hello packets should now be sent to the neighbor at intervals of `HelloInterval` seconds) across all OSPF areas and interfaces.
`n2way`	The sum total number of bidirectional communication establishment between this router and other neighboring routers.
`adjoint ok`	The sum total number of decisions to be made (again) as to whether an adjacency should be established/maintained with the neighbor across all OSPF areas and interfaces.
`negotiation done`	The sum total number of neighbors in this state wherein the Master/slave relationship has been negotiated, and sequence numbers have been exchanged, across all OSPF areas and interfaces.
`exchange done`	The sum total number of neighbors in this state (that is, in an adjacency's final state) having transmitted a full sequence of Database Description packets, across all OSPF areas and interfaces.
`bad requests`	The sum total number of Link State Requests which have been received for a link state advertisement not contained in the database across all interfaces and OSPF areas.

Table 82 OSPF Interface Statistics

Statistic	Description
`bad sequence`	The sum total number of Database Description packets which have been received that either: a. Has an unexpected DD sequence number b. Unexpectedly has the init bit set c. Has an options field differing from the last Options field received in a Database Description packet. Any of these conditions indicate that some error has occurred during adjacency establishment for all OSPF areas and interfaces.
`loading done`	The sum total number of link state updates received for all out-of-date portions of the database across all OSPF areas and interfaces.
`n1way`	The sum total number of Hello packets received from neighbors, in which this router is not mentioned across all OSPF interfaces and areas.
`rst_ad`	The sum total number of times the Neighbor adjacency has been reset across all OPSF areas and interfaces.
`down`	The total number of Neighboring routers down (that is, in the initial state of a neighbor conversation) across all OSPF areas and interfaces.
OSPF Interface Change Statistics	
`hello`	The sum total number of Hello packets sent on all interfaces and areas.
`down`	The sum total number of interfaces down in all OSPF areas.
`loop`	The sum total of interfaces no longer connected to the attached network across all OSPF areas and interfaces.
`unloop`	The sum total number of interfaces, connected to the attached network in all OSPF areas.
`wait timer`	The sum total number of times the Wait Timer has been fired, indicating the end of the waiting period that is required before electing a (Backup) Designated Router across all OSPF areas and interfaces.
`backup`	The sum total number of Backup Designated Routers on the attached network for all OSPF areas and interfaces.
`nbr change`	The sum total number of changes in the set of bidirectional neighbors associated with any interface across all OSPF areas.

RIP Statistics

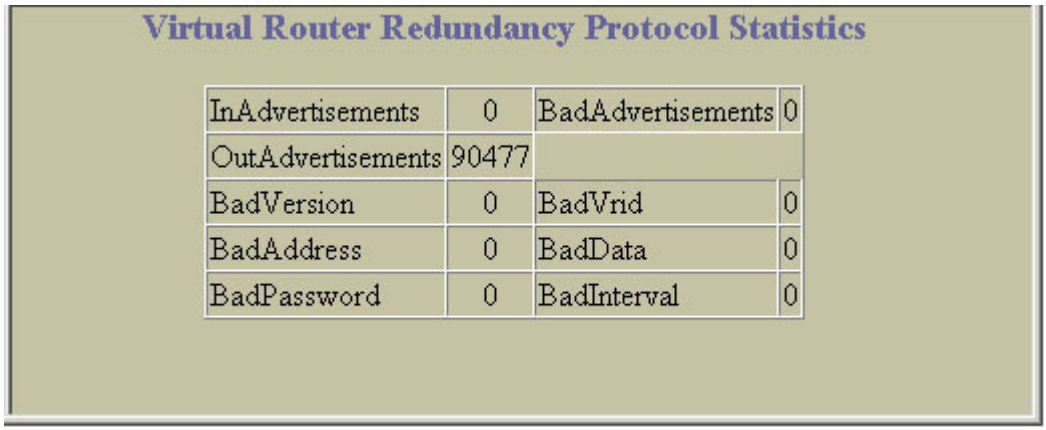
To display the following form, select **Layer 3 > RIP > General**.



This form provides basic Routing Information Protocol statistics.

Virtual Router Redundancy Protocol Statistics

To display the following form, select **Layer 3 > VRRP > General**.



The following table describes VRRP statistics:

Table 83 Virtual Router Redundancy Protocol Statistics

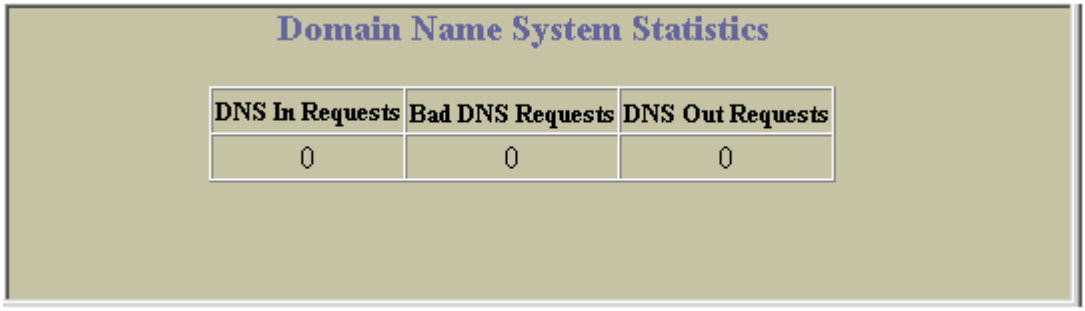
Statistic	Description
`InAdvertisements`	The total number of VRRP advertisements that have been received.
`BadAdvertisements`	The total number of VRRP advertisements received that were dropped.
`OutAdvertisements`	The total number of VRRP advertisements that have been sent.
`BadVersion`	The total number of VRRP advertisements that had a bad version number.
`BadVrid`	The total number of VRRP advertisements that had a bad virtual router ID.
`BadAddress`	The total number of VRRP advertisements that had a bad address.
`BadData`	The total number of VRRP advertisements that had bad data.

Table 83 Virtual Router Redundancy Protocol Statistics

Statistic	Description
`BadPassword`	The total number of VRRP advertisements that had a bad password.
`BadInterval`	The total number of VRRP advertisements that had a bad interval.

Domain Name System Statistics

To display the following form, select **IP Menu > Domain Name System**.



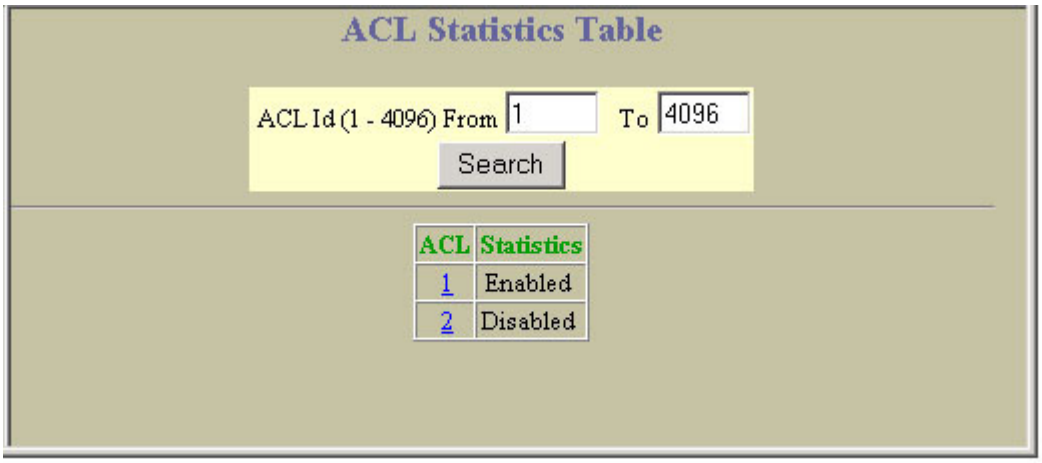
The following table describes DNS statistics:

Table 84 DNS Statistics

Statistic	Description
DNS In Requests	The total number of DNS request packets that have been received.
Bad DNS Requests	The total number of DNS request packets received that were dropped.
DNS Out Requests	The total number of DNS response packets that have been transmitted.

ACL Statistics

To display the following form, select **Access Control > Access Control Lists** (click the underlined text, not the folder).

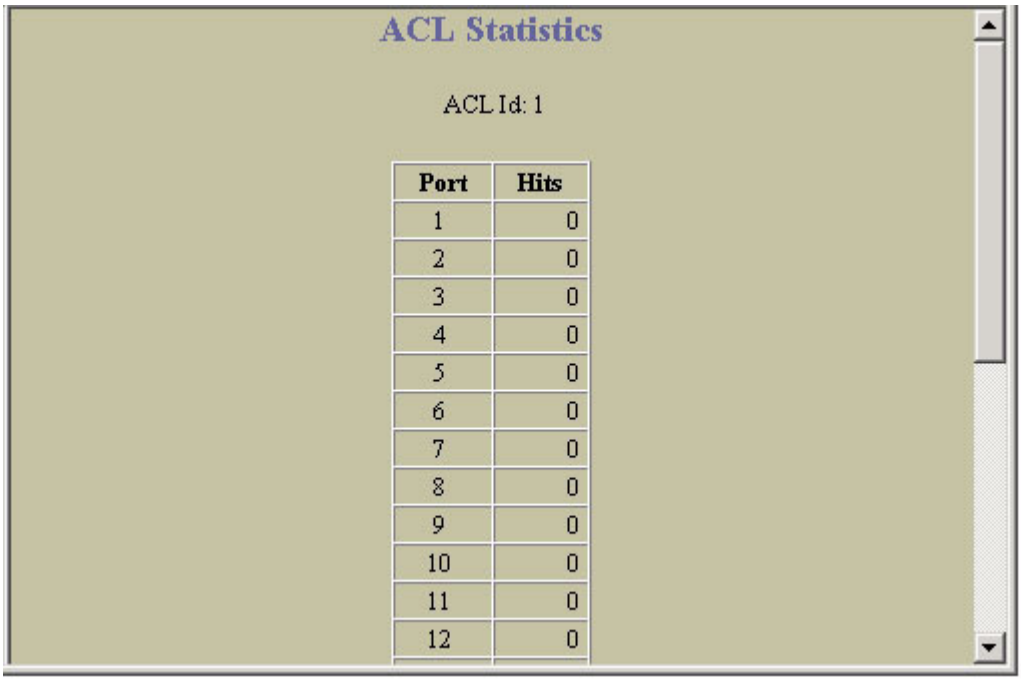


The following table describes ACL statistics:

Table 85 ACL Statistics

Statistic	Description
Search	Enter a range of ACL numbers and click search to display them in the list of ACLs.
ACL	Displays ACL numbers.
Statistics	Shows whether ACL statistics is enabled or disabled.

To display the following form, go to the ACL Statistics table. Select an ACL number.



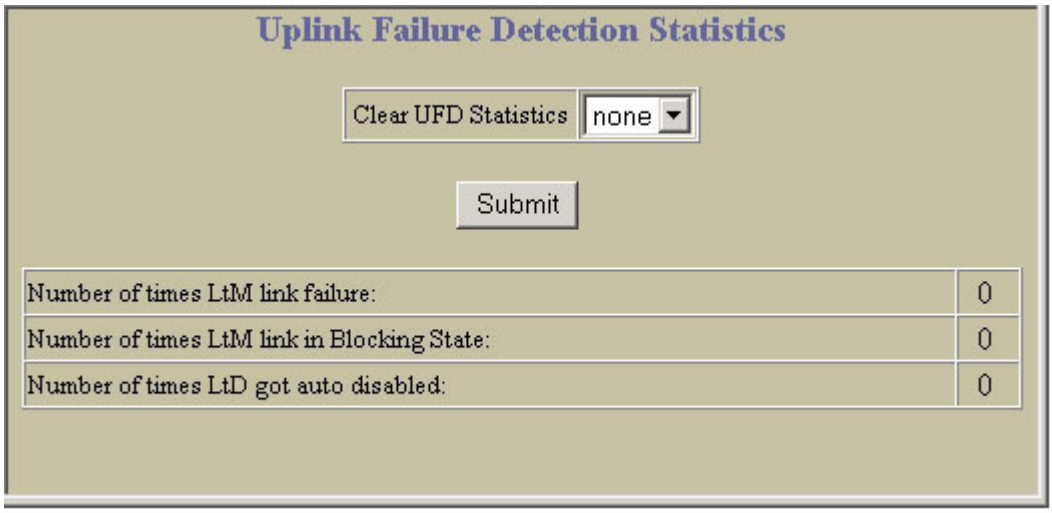
The following table describes ACL statistics:

Table 86 ACL Statistics

Statistic	Description
Port	Displays the port number.
Hits	Shows the number of times the ACL was activated on the port.

Uplink Failure Detection Statistics

To display the following form, select **Uplink Failure Detection** (click the underlined text, not the folder).



The following table describes commands for Uplink Failure Detection (UFD) statistics:

Table 87 Uplink Failure Detection Statistics

Control	Description
Clear UFD Statistics	To clear UFD statistics, select `clear` in the drop-down list, and click **Submit**.
Number of times LtM link failure	The total number of times that link failures were detected on the uplink ports in the Link to Monitor group.
Number of times LtM link in Blocking State	The total number of times that Spanning Tree Blocking state was detected on the uplink ports in the Link to Monitor group.
Number of times LtD got auto disabled	The total number of times that downlink ports in the Link to Disable group were automatically disabled because of a failure in the Link to Monitor group.

Configuring the switch

Introduction

The GbE2 Interconnect Switch BBI can be used to view and change switch configuration parameters. The same configuration parameters that are available through the switch's command-line interface are present on the BBI configuration forms.

The following provides a basic outline for GbE2 Interconnect Switch configuration. You should first be familiar with configuration as covered in the *HP ProLiant BL p-Class GbE2 Interconnect Switch Command Reference Guide*.

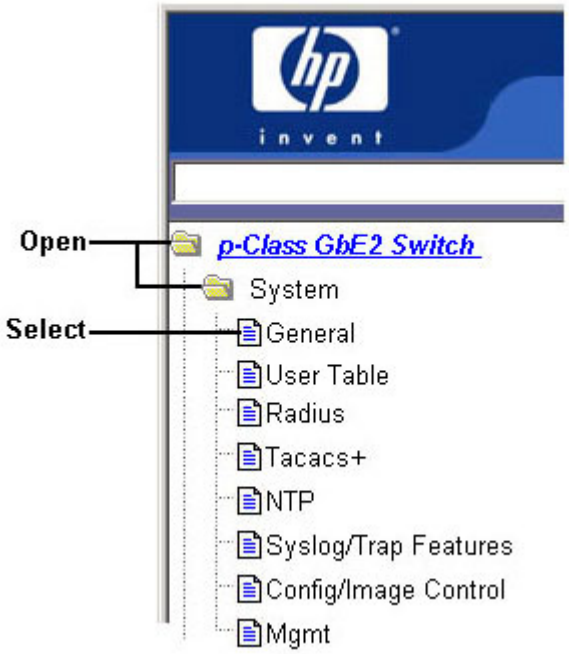
IMPORTANT: You must be logged in using the administrator account in order to change GbE2 Interconnect Switch configuration settings.

Configuration steps

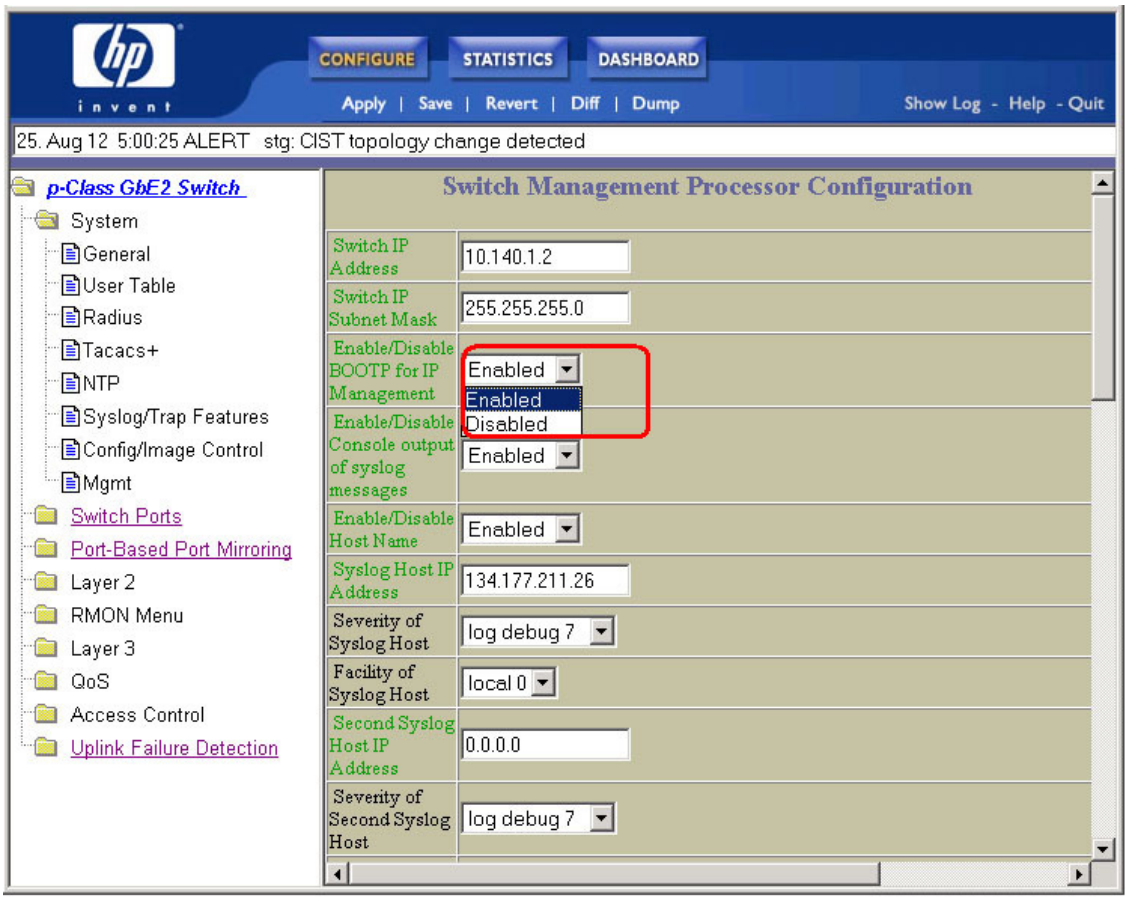
Follow these basic steps for viewing or configuring GbE2 Interconnect Switch parameters:

1. Select the **Configure** context button in the toolbar.

2. Select a feature icon in the navigation window. For example:



3. View or make changes to the settings shown in the forms window. For example:

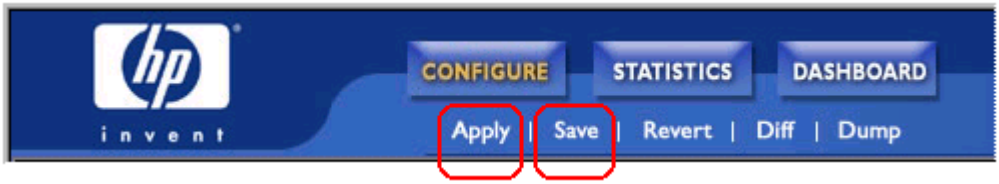


NOTE: Fields, which must be configured for proper GbE2 Interconnect Switch operations, are highlighted on the forms in green type. Items which load other forms when selected are underlined.

4. Submit the form contents using the button on the bottom of the form.

Button	Description
Submit	When selected, the form is sent to the GbE2 Interconnect Switch. Any configuration changes are placed in the "pending" state and do not take effect until the toolbar **Apply** command is given.

5. Apply and save your changes using the toolbar commands.



Pending configuration changes (including deletions) do not take effect until the **Apply** command is selected. You can view pending changes on the Configuration form, but they do not appear on the Dashboard. The Dashboard displays the current active (applied) configuration.

Applied changes take effect on the GbE2 Interconnect Switch immediately, but are lost the next time the switch is rebooted, unless the **Save** command is selected. When you click **Save**, you have two save options: **Save** and **Save n**. With **Save**, your new configuration changes are placed in the **active** configuration block. The previous configuration is copied into the **backup** configuration block. If you select **Save n**, your new configuration changes are placed in the **active** configuration block, and the **backup** configuration block remains unchanged.

Input error checking

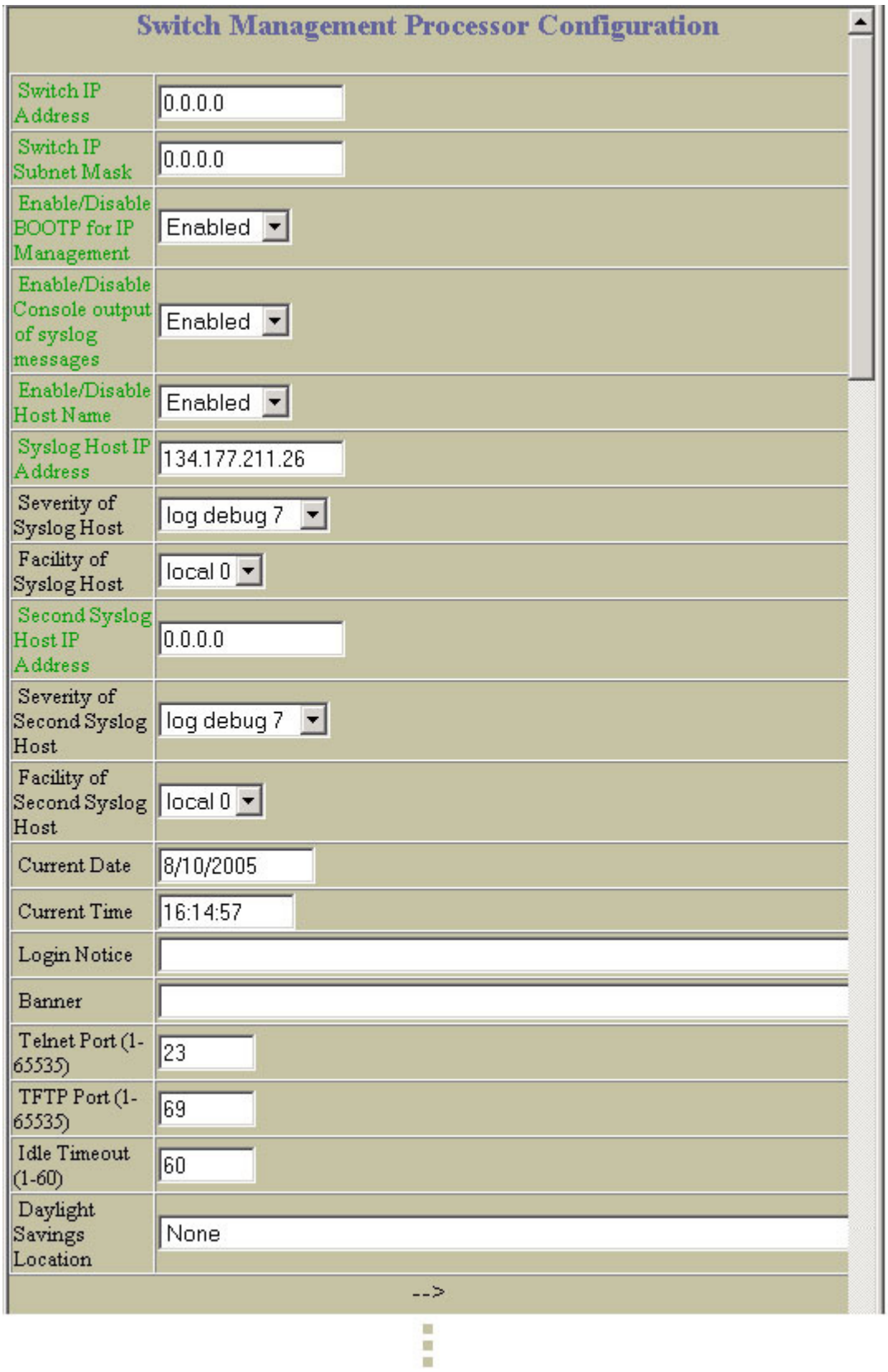
The BBI performs two levels of input error-checking, as follows:

- **Submit**: When you click **Submit** on a Configuration form, the BBI checks the format and range of pending configuration changes. For example, if you enter a value that is out of range (VLAN = 8097), a log error is generated.
- **Apply**: When you click **Apply** to make pending changes active, the switch checks the validity of pending configuration changes. For example, an invalid MIB OID can pass the format check during Submit, if the format is correct. The invalid OID is rejected when you attempt to apply the configuration.

Switch Management Processor Configuration

Basic system configuration

To display the following form, select **System > General**.



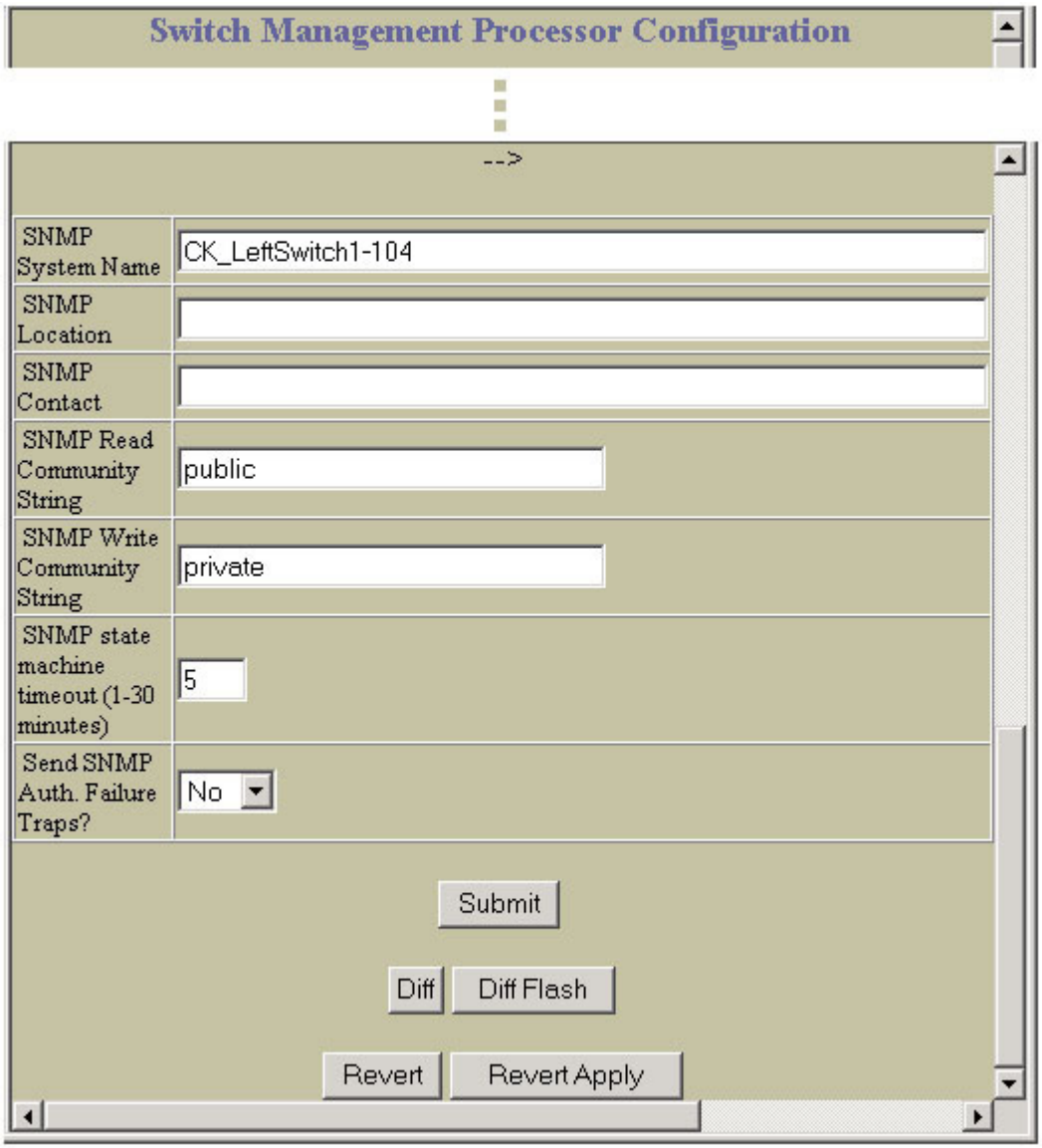
The following table describes the Switch Management Processor Configuration (basic) controls:

Table 88 Switch Management Processor Configuration (Basic) controls

Control	Description
Switch IP Address	Configures the IP address of the switch interface using dotted decimal notation.
Switch IP Subnet Mask	Configures the IP subnet address mask for the interface using dotted decimal notation.
Enable/Disable BOOTP for IP Management	Enables or disables the use of `BOOTP`. If you enable `BOOTP`, the switch will query its `BOOTP` server for all of the switch IP parameters. This command is enabled by default.
Enable/Disable Console output of syslog messages	Enables or disables delivering syslog messages to the console. When necessary, disabling console ensures the switch is not affected by syslog messages. It is enabled by default.
Enable/Disable Host Name	Enables or disables displaying of the host name (system administrator's name) in the Command Line Interface (CLI).
Syslog Host IP Address	Sets the IP address of the first syslog host.
Severity of Syslog Host	This option sets the severity level of the first syslog host displayed. The default is 7, which means log all the seven severity levels.
Facility of Syslog Host	This option sets the facility level of the first syslog host displayed. The default is 0.
Second Syslog Host IP Address	Sets the IP address of the second syslog host.
Severity of Second Syslog Host	This option sets the severity level of the second syslog host displayed. The default is 7, which means, log all seven severity levels.
Facility of Second Syslog Host	This option sets the facility level of the second syslog host displayed. The default is 0.
Current Date	Configures the system date.
Current Time	Configures the system time using a 24-hour clock format.
Login Notice	Displays login notice immediately before the "Enter password:" prompt in the Command Line Interface (CLI). This notice can contain up to 1024 characters and new lines.
Banner	Configures a login banner of up to 80 characters. When a user or administrator logs into the switch Command Line Interface (CLI), the login banner is displayed. It is also displayed as part of the output from the `/info/sys/gen` command.
Telnet Port (1-65535)	Sets an optional telnet server port number for cases where the server listens for telnet sessions on a non-standard port. The default is 23.
TFTP Port (1-65535)	Sets an optional TFTP server port number for cases where the server listens for TFTP sessions on a non-standard port. The default is 69.
Idle Timeout (1-60)	Sets the idle timeout for CLI sessions, from 1 to 60 minutes. The default is 5 minutes.
Daylight Savings Location	Configures the time zone where the switch resides. You are prompted to select your location (continent, country, region) by the timezone wizard. Once a region is selected, the switch updates the time to reflect local changes to Daylight Savings Time, etc.

SNMP controls

To display the following form, select **System > General**.



The following table describes the Switch Management Processor Configuration (SNMP) controls:

Table 89 Switch Management Processor Configuration (SNMP) controls

Control	Description
SNMP System Name	Configures the name for the system. The name can have a maximum of 32 characters.
SNMP Location	Configures the name of the system location. The location can have a maximum of 32 characters.
SNMP Contact	Configures the name of the system contact. The contact can have a maximum of 32 characters.
SNMP Read Community String	Configures the SNMP read community string. The read community string controls SNMP "get" access to the switch. It can have a maximum of 32 characters. The default read community string is **public**.
SNMP Write Community String	Configures the SNMP write community string. The write community string controls SNMP "set" and "get" access to the switch. It can have a maximum of 32 characters. The default write community string is **private**.
SNMP state machine timeout (1-30 minutes)	Sets the timeout value for the SNMP state machine.

Table 89 Switch Management Processor Configuration (SNMP) controls

Control	Description
Send SNMP Auth. Failure Traps?	Enables or disables the use of the system authentication trap facility. The default setting is disabled.

Switch Management Processor Configuration buttons

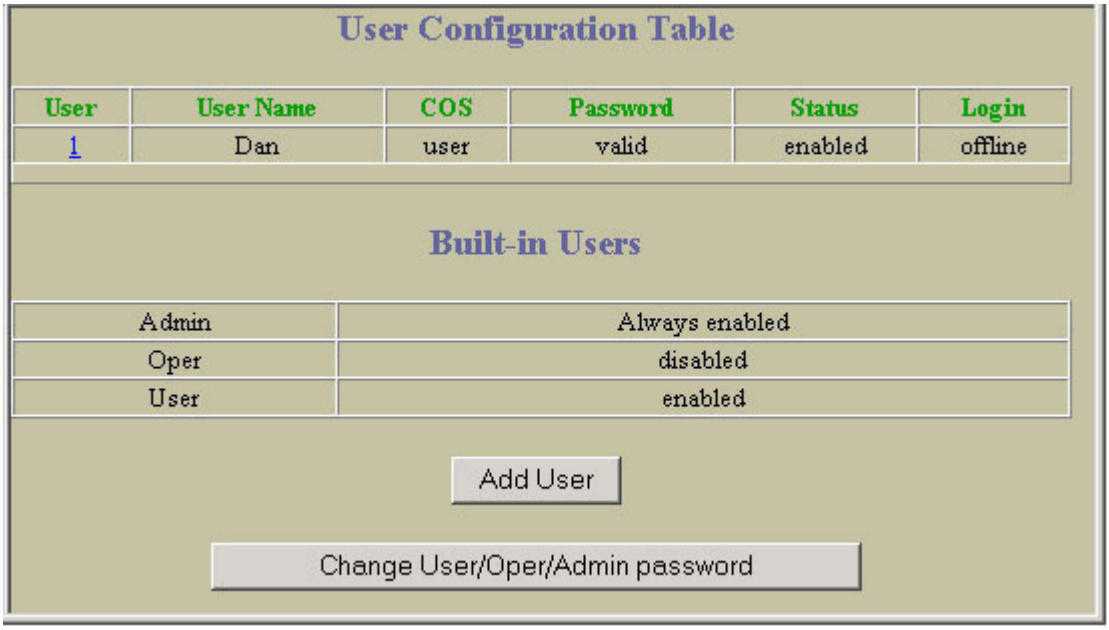
The following table describes the Switch Management Processor Configuration buttons:

Table 90 Switch Management Processor Configuration buttons

Control	Description
Submit	Sends this form to the GbE2 Interconnect Switch. Any configuration changes are placed in the "pending" state and do not take effect until the toolbar **Apply** command is given.
Diff	Shows any pending configuration changes.
Diff Flash	Compares new configuration with the flash configuration.
Revert	Removes pending configuration changes between **apply** commands. Use this command to restore configuration parameters set since last **apply** command.
Revert Apply	Removes pending configuration changes between **save** commands. Use this command to restore configuration parameters set since last **save** command.

User Configuration Table

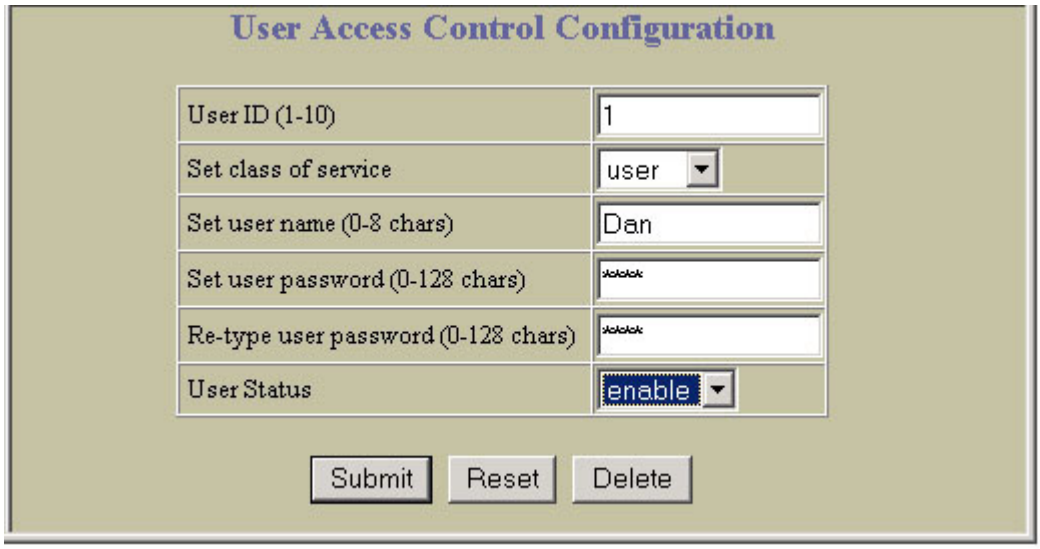
To display the following form, select **System > User Table**.



This form summarizes the users configured on the GbE2 Interconnect Switch. Click **Add User** to define a new user. Click **Change User/Oper/Admin password** to configure new passwords for the switch.

User Access Control Configuration

To display the following form, go to the User Configuration Table and click **Add User**.



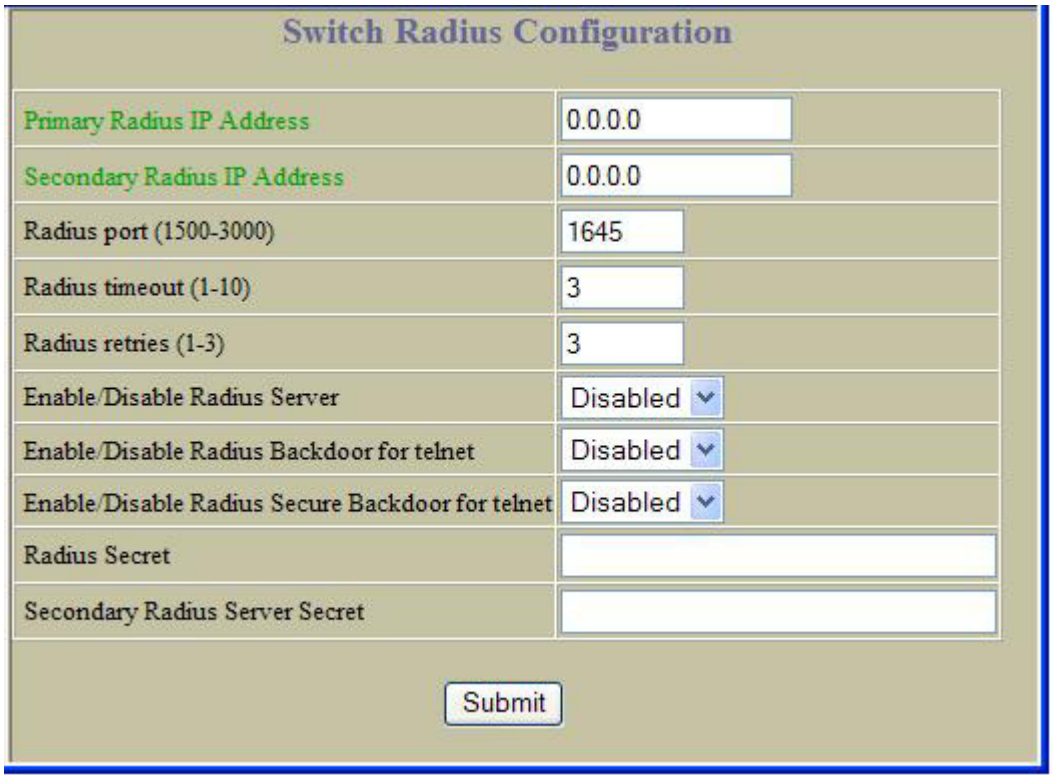
The following table describes User Access Configuration controls:

Table 91 User Access Configuration controls

Control	Description
User ID (1-10)	Sets a numeric identifier for the user.
Set Class of Service	Sets the Class-of-Service to define the user's authority level.
Set user name (0-8 chars)	Defines the user name of maximum eight characters.
Set user password (0-128 chars)	Sets the user password of up to 128 characters maximum.
Re-type user password (0-128 chars)	Confirms the user password.
User Status	Enables or disables the user.

Switch RADIUS Configuration

To display the following form, select **System > Radius**.



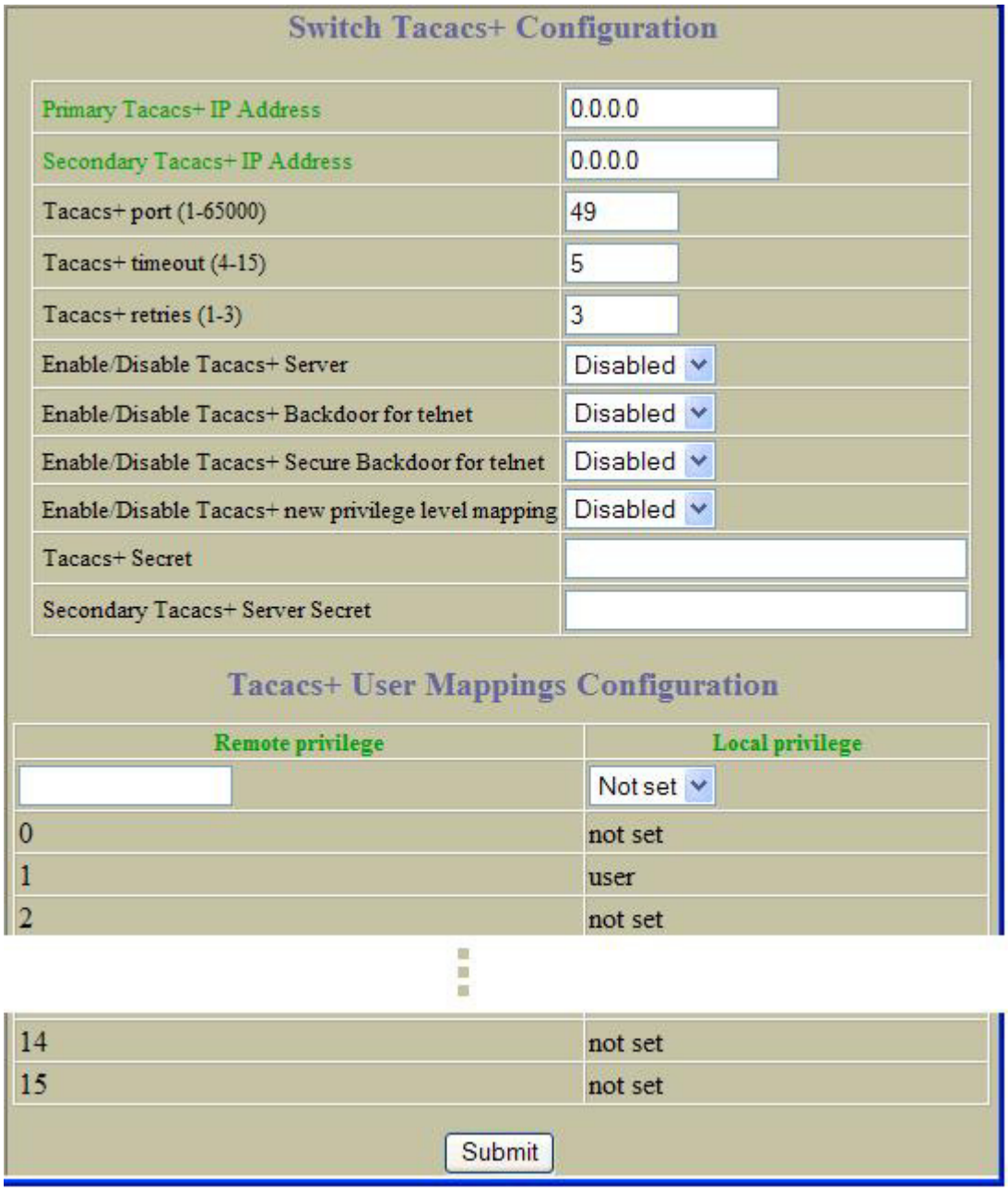
The following table describes Switch Radius Configuration controls:

Table 92 Switch RADIUS Configuration controls

Control	Description
Primary Radius IP Address	Configures the primary Radius server address.
Secondary Radius IP Address	Configures the secondary Radius server address.
Radius port (1500-3000)	Configures the number of the UDP port to be configured, between 1500 - 3000. The default is 1645.
Radius timeout (1-10)	Configures the amount of time, in seconds, before a Radius server authentication attempt is considered to have failed. The default is 3 seconds.
Radius retries (1-3)	Configures the number of failed authentication requests before switching to a different Radius server. The default is 3 requests.
Enable/Disable Radius Server	Enables or disables the Radius server.
Enable/Disable Radius Backdoor for telnet	Enables or disables the RADIUS back door for telnet/SSH/ HTTP/HTTPS. This command does not apply when secure backdoor is enabled.
Enable/Disable Radius Secure Backdoor for telnet	Enables or disables the RADIUS back door using secure password for telnet/SSH/ HTTP/HTTPS.
Radius Secret	Defines the shared secret (up to 32 characters) between the switch and the RADIUS server(s).
Secondary Radius Server Secret	Defines the secondary shared secret (up to 32 characters) between the switch and the Radius server(s).

Switch TACACS+ Configuration

To display the following form, select **System > Tacacs+**.



TACACS+ (Terminal Access Controller Access Control System) is an authentication protocol that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system. TACACS+ and Remote Authentication Dial-In User Service (RADIUS) protocols are more secure than the TACACS encryption protocol. TACACS+ is described in RFC 1492.

TACACS+ protocol is more reliable than RADIUS, as TACACS+ uses the Transmission Control Protocol (TCP) whereas RADIUS uses the User Datagram Protocol (UDP). Also, RADIUS combines authentication and authorization in a user profile, whereas TACACS+ separates the two operations.

TACACS+ offers the following advantages over RADIUS as the authentication device:

- TACACS+ is TCP-based, so it facilitates connection-oriented traffic.
- It supports full-packet encryption, as opposed to password-only in authentication requests.
- It supports decoupled authentication, authorization, and accounting.

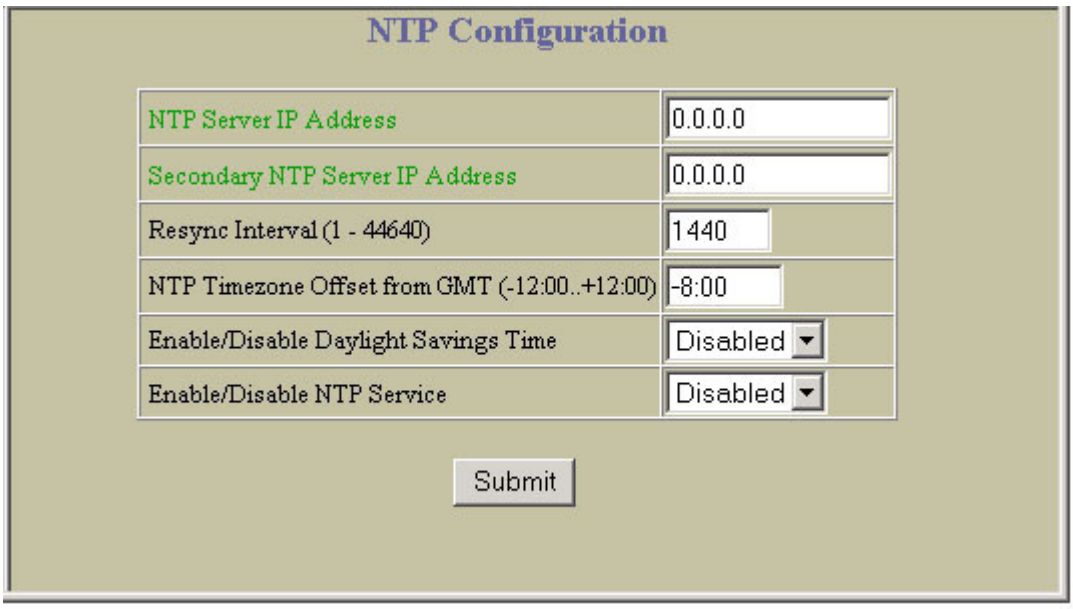
The following table describes Switch TACACS+ Configuration controls:

Table 93 Switch TACACS+ Configuration controls

Control	Description
Primary Tacacs+ IP Address	Configures the primary TACACS+ server address.
Secondary Tacacs+ IP Address	Configures the secondary TACACS+ server address.
Tacacs+ port (1-65000)	Configures the number of the TCP port to be configured, between 1 and 65000. The default is 49.
Tacacs+ timeout (4-15)	Configures the amount of time, in seconds, before a TACACS+ server authentication attempt is considered to have failed. The default timeout is 5 seconds.
Tacacs+ retries (1-3)	Configures the number of failed authentication requests before switching to a different TACACS+ server. The default retry count is 3 requests.
Enable/Disable Tacacs+ Server	Enables or disables the Tacacs+ server.
Enable/Disable Tacacs+ Backdoor for telnet	Enables or disables the Tacacs+ backdoor for telnet. Telnet also applies to SSH/SCP connections.
Enable/Disable Tacacs+ new privilege level mapping	Enables or disables TACACS+ privilege-level mapping. The default value is `disabled`.
Tacacs+ Secret	Configures the shared secret (up to 32 characters) between the switch and the TACACS+ server.
Secondary Tacacs+ Server Secret	Configures the secondary shared secret (up to 32 characters) between the switch and the TACACS+ server.
Tacacs+ User Mappings Configuration	Maps a TACACS+ privilege level to a GbE2 user level, as follows: **Remote Privilege** Enter a TACACS+ privilege level (0-15) **Local Privilege** Select the corresponding GbE2 user level.

NTP Configuration

To display the following form, select **System > NTP**.



This form enables you to synchronize the switch clock to a Network Time Protocol (NTP) server. By default, this option is disabled.

The following table describes NTP Configuration controls:

Table 94 NTP Configuration controls

Control	Description
NTP Server IP Address	Configures the IP address of the primary NTP server to which you want to synchronize the switch clock.
Secondary NTP Server IP Address	Configures the IP address of the secondary NTP server to which you want to synchronize the switch clock.
Resync Interval (1-44640)	Specifies the interval, that is, how often, in minutes (1-44640), to re-synchronize the switch clock with the NTP server.
NTP Timezone Offset from GMT(-12:00...+12:00)	Configures the NTP time zone offset, in hours and minutes, of the switch you are synchronizing from Greenwich Mean Time (GMT).
Enable/Disable Daylight Savings Time	Disables or enables daylight savings time in the system clock. When enabled, the switch will add an extra hour to the system clock so that it is consistent with the local clock. By default, this option is disabled.
Enable/Disable NTP Service	Enables or disables the NTP synchronization service.

Syslog and Trap Feature Configuration

To display the following form, select **System > Syslog/Trap Features**.

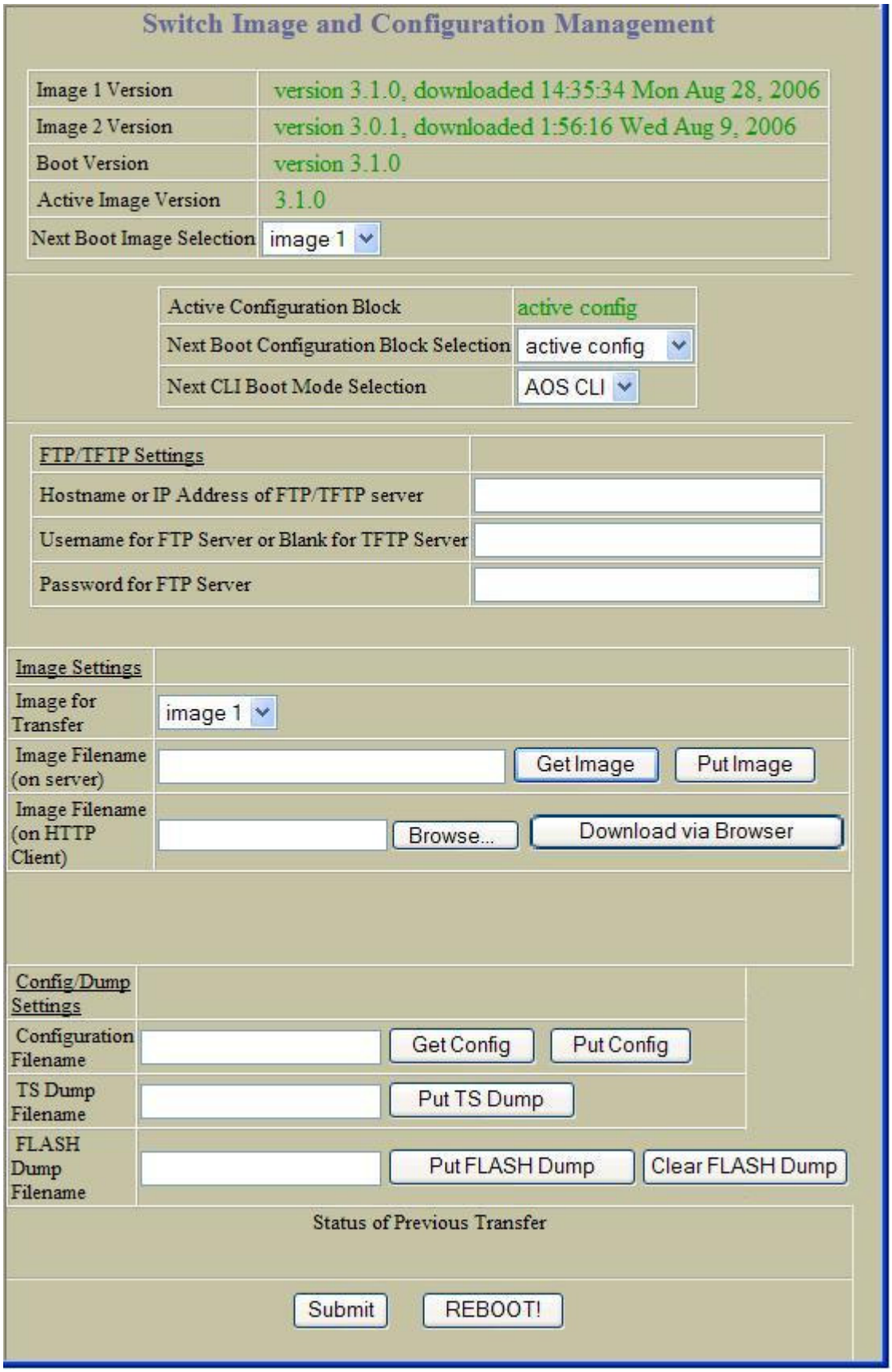
The following table describes Syslog and Trap Feature Configuration controls:

Table 95 Syslog and Trap Feature Configuration controls

Control	Description
Enable/Disable Syslog and Trap of Console	Enables or disables syslog messages and traps of console-related events.
Enable/Disable Syslog and Trap of System	Enables or disables syslog messages and traps of system-related events.
Enable/Disable Syslog and Trap of Management	Enables or disables syslog messages and traps of management-related events.
Enable/Disable Syslog and Trap of CLI	Enables or disables syslog messages and traps of CLI-related events.
Enable/Disable Syslog and Trap of STP	Enables or disables syslog messages and traps of STP-related events.
Enable/Disable Syslog and Trap of VLAN	Enables or disables syslog messages and traps of VLAN-related events.
Enable/Disable Syslog and Trap of WEB	Enables or disables syslog messages and traps of Web-related events.
Enable/Disable Syslog and Trap of IP	Enables or disables syslog messages and traps of IP-related events.
Enable/Disable Syslog and Trap of VRRP	Enables or disables syslog messages and traps of VRRP-related events.
Enable/Disable Syslog and Trap of SSH	Enables or disables syslog messages and traps of SSH-related events.
Enable/Disable Syslog and Trap of NTP	Enables or disables syslog messages and traps of NTP-related events.
Enable/Disable Syslog and Trap of OSPF	Enables or disables syslog messages and traps of OSPF-related events.
Enable/Disable Syslog and Trap of RMON	Enables or disables syslog messages and traps of Remote Monitoring (RMON) events.
Enable/Disable Syslog and Trap of 802.1x	Enables or disables syslog messages and traps of 802.1x-related events.
Enable/Disable Syslog of UFD	Enables or disables syslog messages of Uplink Failure Detection (UFD) events.
Enable/Disable Syslog of CFG	Enables or disables syslog messages of configuration events.
Enable/Disable Trap of UFD	Enables or disables event traps of Uplink Failure Detection (UFD) events.

Switch Image and Configuration Management

To display the following form, select **System > Config/Image Control**.



The switch software image is the executable code running on the GbE2 Interconnect Switch. A version of the image ships with the switch, and comes pre-installed on the device. As new versions of the image are released, you can upgrade the software running on your switch.

Upgrading the software image on your switch requires the following:

- Loading the new image onto a FTP/TFTP server on your network
- Downloading the new image from the FTP/TFTP server to your switch
- Selecting the new software image to be loaded into switch memory the next time the switch is reset

Downloading new software to your switch

The switch can store up to two different software images, called `image1` and `image2`, as well as boot software, called `boot`. When you download new software, you must specify where it should be placed: either into `image1`, `image2`, or `boot`.

For example, if your active image is currently loaded into `image1`, you would probably load the new image software into `image2`. This lets you test the new software and reload the original active image (stored in `image1`), if needed.

To download new software to your switch, you will need the following:

- The image or boot software loaded on a FTP/TFTP server on your network
- The hostname or IP address of the FTP/TFTP server
- The name of the new software image or boot file

Configuration

When you make configuration changes to the GbE2 Interconnect Switch, you must save the changes so that they are retained beyond the next time the switch is reset. When you perform the `save` command, you have two save options: **save** and **save n**. With **save**, your new configuration changes are placed in the **active** configuration block. The previous configuration is copied into the **backup** configuration block. If you select **save n**, your new configuration changes are placed in the **active** configuration block, and the **backup** configuration block remains unchanged.

There is also a **factory** configuration block. This holds the default configuration set by the factory when your GbE2 Interconnect Switch was manufactured. Under certain circumstances, it may be desirable to reset the switch configuration to the default. This can be useful when a custom-configured GbE2 Interconnect Switch is moved to a network environment where it will be re configured for a different purpose.

Switch Image and Configuration Management controls

The following table describes Switch Image and Configuration Management controls:

Table 96 Switch Image and Configuration Management controls

Control	Description
Image 1 Version	Displays information about the current Image 1 software.
Image 2 Version	Displays information about the current Image 2 software.
Boot Version	Displays the version number of the current Boot software.
Active Image Version	Displays the version number of the active software image.
Next Boot Image Selection	Selects which software image (`image1` or `image2`) you want to run in switch memory for the next reboot.
Active Configuration Block	Displays the Configuration Block file that is currently running (active or backup).
Next Boot Configuration Block Selection	Selects the Configuration Block file (active or backup) that will run after the next reboot.
Next CLI Boot Mode Selection	Selects the type of command-line interface (CLI) used after the next reboot.
FTP/TFTP Settings	
Hostname or IP Address of FTP/TFTP server	Enter the host name or IP address of the FTP/TFPT server from which you will download software.
Username for FTP Server or Blank for TFTP Server	Enter the user name for the FTP server, if required.

Table 96 Switch Image and Configuration Management controls

Control	Description
Password for FTP Server	Enter the password for the FTP server, if required.
Image Settings	
Image for Transfer	Selects a software image to replace with the downloaded software.
Image Filename (on server)	Enter the name of the file on a FTP/TFTP server that contains the software image you want to download.
Image Filename (on HTTP Client)	Enter the name of the file on an HTTP Client that contains the software image you want to download.
Config/Dump Settings	
Configuration Filename	Selects the file name and location of the Configuration Block file to be downloaded.
TS Dump Filename	Selects the filename for the TS (tech support) dump that you want to upload to the FTP/TFTP server.
Flash Dump Filename	Selects the filename for the core (PANIC) dump that you want to upload to the FTP/TFTP server.
Status of Previous Transfer	Displays the status of the previous software download attempt.

Switch Image and Configuration Management buttons

The following table describes Switch Image and Configuration Management buttons:

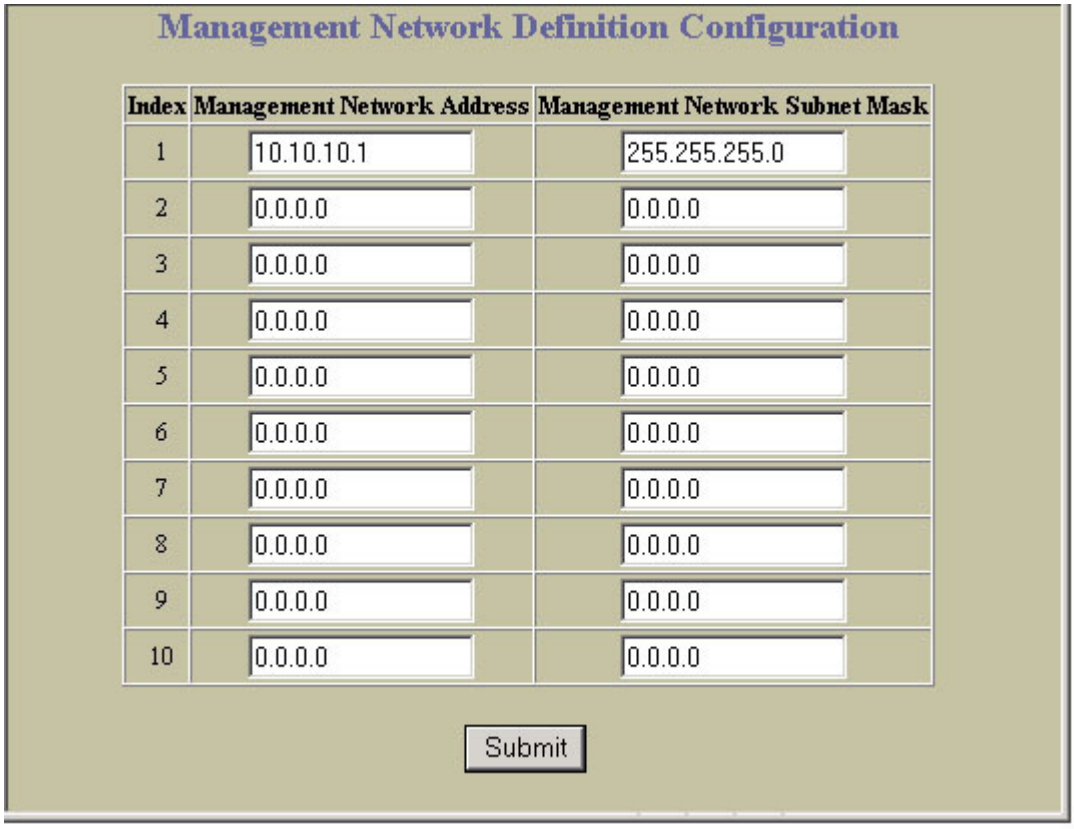
Table 97 Switch Image and Configuration Management buttons

Button	Description
Get Image	Starts download of the software image file indicated in TFTP Image Filename field from the specified TFTP server.
Put Image	Starts upload of the software image file indicated in TFTP Image Filename field from the specified TFTP server.
Get Config	Downloads a previously saved switch Configuration Block file indicated in Configuration Filename from the specified the FTP/TFTP server. The active configuration will be replaced with the commands found in the downloaded configuration file. The file can contain a full switch configuration or a partial switch configuration. The new configuration is not activated until the **apply** command is used. If the **apply** command is found in the configuration script file loaded using this command, the **apply** action is performed automatically.
Put Config	Uploads the switch's active configuration to the script configuration file specified in Configuration Filename. The file is placed on the FTP/TFTP server.
Put TS Dump	Uploads the TS (tech support) dump file to the FTP/TFTP server specified in TSTP TS Dump Filename.
Put Dump	Uploads the core (PANIC) dump file to the FTP/TFTP server specified in Core Dump Filename.
Clear Flash Dump	Deletes the core dump in flash memory.
Submit	When selected, the form is sent to the GbE2 Interconnect Switch. Any configuration changes are placed in the "pending" state and do not take effect until the toolbar **Apply** command is given.
REBOOT!	Reboots the switch.

NOTE: If the FTP/TFTP server is running SunOS or the Solaris operating system, the specified Put Config file must exist prior to executing the **Put Config** command and must be writable (set with proper permission, and not locked by any application). The contents of the specified file will be replaced with the current configuration data.

Management Network Definition Configuration

To display the following form, select **System > Mgmt**.



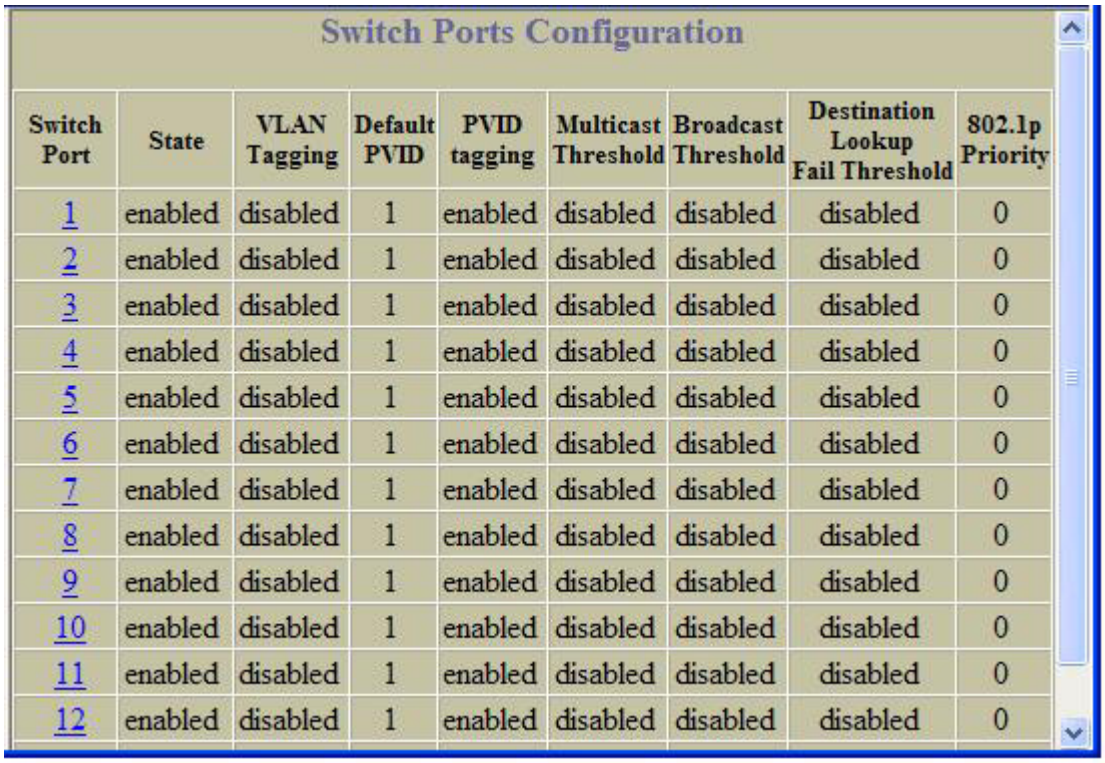
The following table describes the Management Network Definition Configuration controls:

Table 98 Management Network Definition Configuration controls

Control	Description
Index	Displays the index number that identifies each management network.
Management Network Address	Adds a defined network through which switch access is allowed through Telnet, SNMP, RIP, or the browser-based interface. A range of IP addresses is produced when used with a network mask address. Specify an IP address in dotted-decimal notation.
Management Network Subnet Mask	Specify a mask address in dotted-decimal notation.

Switch Ports Configuration

To display the following form, select **System > Switch Ports** (click the underlined text, not the folder).



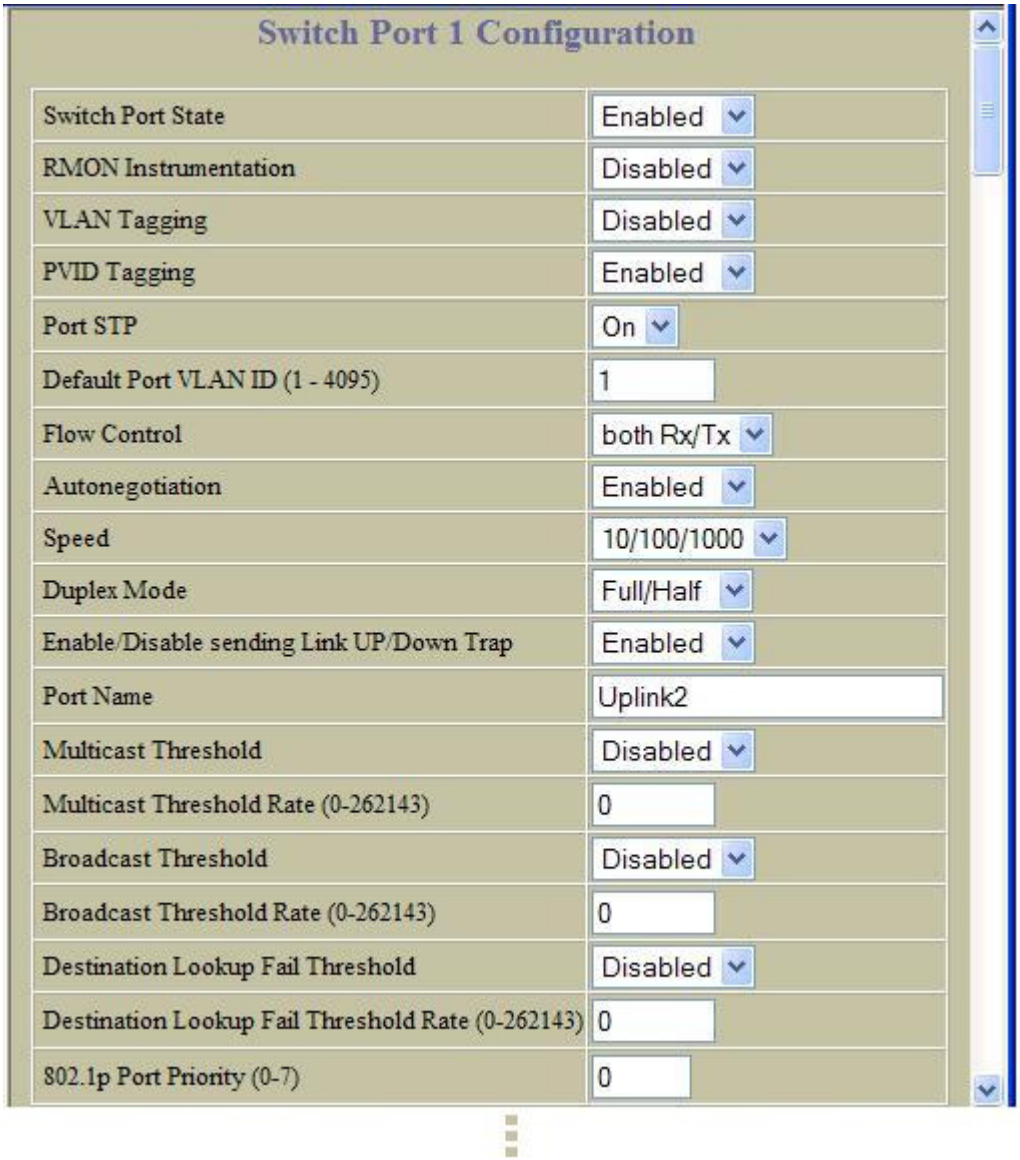
Switch Ports Configuration

Switch Port	State	VLAN Tagging	Default PVID	PVID tagging	Multicast Threshold	Broadcast Threshold	Destination Lookup Fail Threshold	802.1p Priority
1	enabled	disabled	1	enabled	disabled	disabled	disabled	0
2	enabled	disabled	1	enabled	disabled	disabled	disabled	0
3	enabled	disabled	1	enabled	disabled	disabled	disabled	0
4	enabled	disabled	1	enabled	disabled	disabled	disabled	0
5	enabled	disabled	1	enabled	disabled	disabled	disabled	0
6	enabled	disabled	1	enabled	disabled	disabled	disabled	0
7	enabled	disabled	1	enabled	disabled	disabled	disabled	0
8	enabled	disabled	1	enabled	disabled	disabled	disabled	0
9	enabled	disabled	1	enabled	disabled	disabled	disabled	0
10	enabled	disabled	1	enabled	disabled	disabled	disabled	0
11	enabled	disabled	1	enabled	disabled	disabled	disabled	0
12	enabled	disabled	1	enabled	disabled	disabled	disabled	0

This form summarizes the configuration of each port. Select a switch port number to go to its configuration form.

Switch Port Configuration

To display the following form, go to the Switch Ports Configuration form. Select a Switch Port number.



This form allows you to configure settings for individual switch ports.

The following table describes the Switch Port Configuration controls:

Table 99 Switch Port Configuration controls

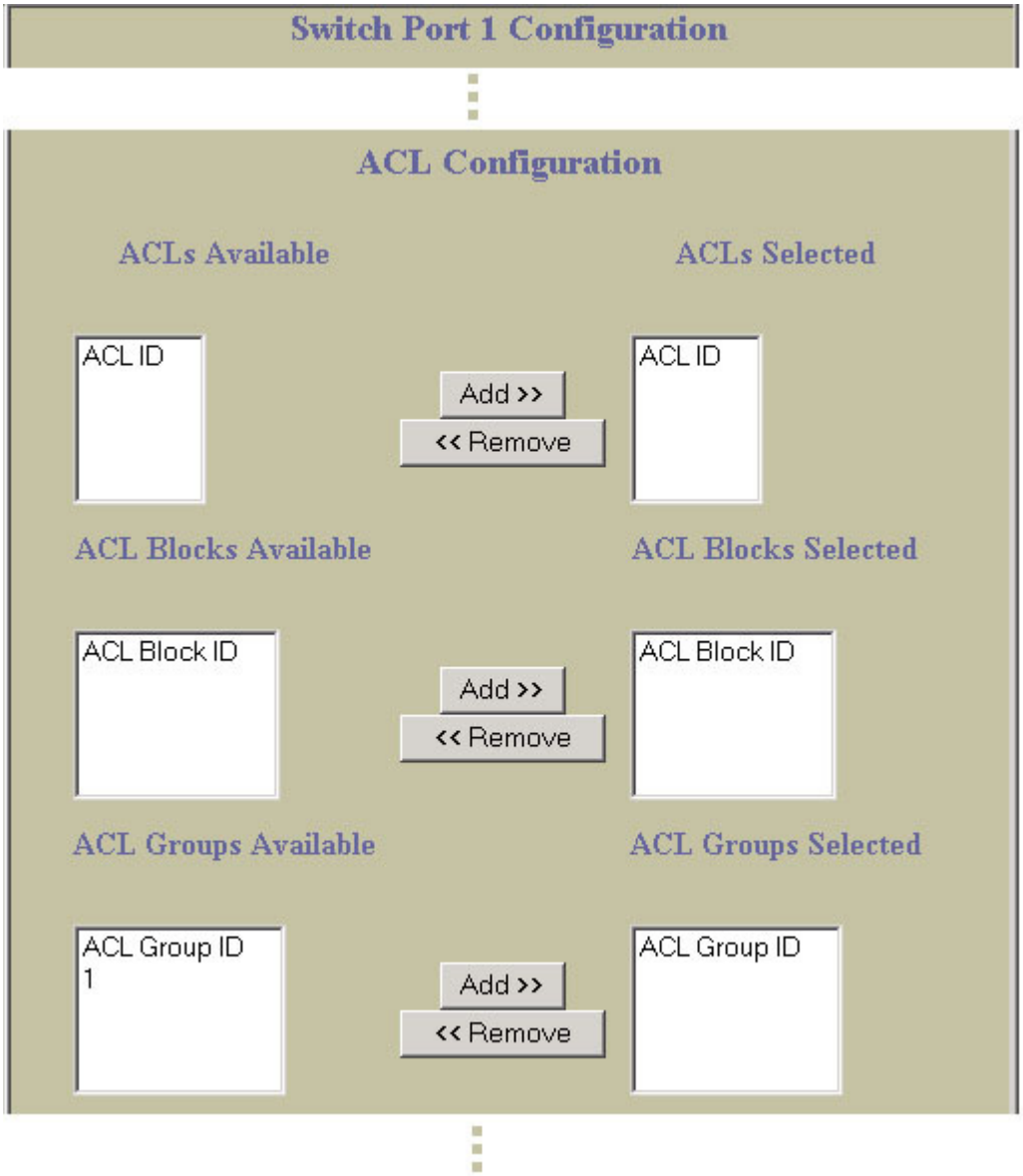
Control	Description
Switch Port State	Enables or disables the port.
RMON Instrumentation	Enables or disables Remote Monitoring for the port. RMON must be enabled for RMON statistics and history sampling to function.
VLAN Tagging	Disables or enables VLAN tagging for this port. It is disabled by default.
PVID Tagging	Disables or enables VLAN tag persistence. When disabled, the VLAN tag is removed from packets whose VLAN tag matches the port PVID. The default value is enabled.
Port STP	Turns Spanning Tree **On** or **Off** for this port.
Default Port VLAN ID (1-4095)	Sets the default VLAN number which will be used to forward frames which are not VLAN tagged. The default number is 1.

Table 99 Switch Port Configuration controls

Control	Description
Flow Control	Sets the flow control. The choices include: • Receive flow control • Transmit flow control • Both receive and transmit flow control (default) • No flow control
Autonegotiation	Enables or disables auto negotiation for the port.
Speed	Sets the link speed. Not all options are valid on all ports. The choices include: • "Any," for automatic detection (default) • 10 Mbps • 100 Mbps • 1000 Mbps
Duplex	Sets the operating mode. The choices include: • "Any," for auto negotiation (default) • Full-duplex • Half-duplex
Enable/Disable sending Link UP/Down Trap	Enables or disables the sending of SNMP link up and link down traps. The default setting is enabled.
Port Name	Sets a name for the port. The assigned port name appears next to the port number on some information and statistics screens.
Multicast Threshold	Enables or disables multicast threshold limit. Limits the number of multicast packets to the specified value. If disabled (`dis`), the port forwards all multicast packets.
Multicast Threshold Rate (0-262143)	Configures the threshold rate for multicast packets, in packets per second.
Broadcast Threshold	Enables or disables broadcast threshold limit. Limits the number of broadcast packets to the specified value. If disabled (`dis`), the port forwards all broadcast packets.
Broadcast Threshold Rate (0-262143)	Configures the threshold rate for broadcast packets, in packets per second.
Destination Look Up Fail Threshold	Enables or disables threshold limit for destination lookup failures. Limits the number of unknown unicast packets to the specified value. If disabled (`dis`), the port forwards all unknown unicast packets.
Destination Lookup Fail Threshold Rate (0-262143)	Configures the threshold rate for destination lookup failures, in packets per second.
802.1p Port Priority (0-7)	Configures the port's 802.1p priority level.

Switch Port ACL Configuration

To display the following form, go to the Switch Ports Configuration form. Select a Switch Port number.



This form allows you to configure Access Control List settings for individual switch ports.

The following table describes the Switch Port ACL Configuration controls:

Table 100 Switch Port ACL Configuration controls

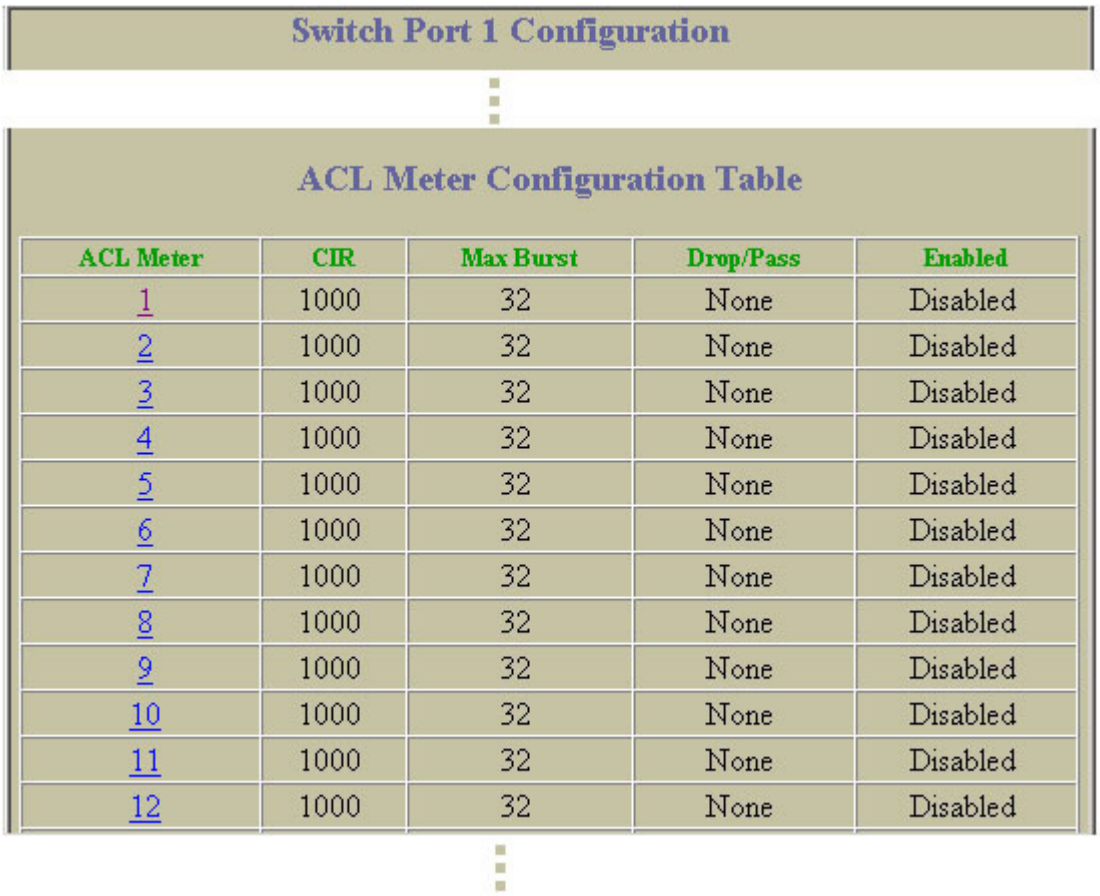
Control	Description
ACLs Available	Lists the ACLs that you can add to the port.
ACLs Selected	Lists the ACLs associated with the port. Select an ACL number in the ACLs Available list, and click **Add** to add the ACL to the port. Select an ACL number in the ACLs Selected list, and click **Remove** to remove the ACL from the port.
ACL Blocks Available	Lists the ACL Blocks that you can add to the port.
ACL Blocks Selected	Lists the ACL Blocks associated with the port. Select an ACL Block number in the ACL Blocks Available list, and click **Add** to add the ACL Block to the port. Select an ACL Block number in the ACL Blocks Selected list, and click **Remove** to remove the ACL Block from the port.
ACL Groups Available	Lists the ACL Groups that you can add to the port.

Table 100 Switch Port ACL Configuration controls

Control	Description
ACL Groups Selected	Lists the ACL Groups associated with the port. Select an ACL Group number in the ACL Groups Available list, and click **Add** to add the ACL Group to the port. Select an ACL Group number in the ACL Groups Selected list, and click **Remove** to remove the ACL Group from the port.

Switch Port ACL Meter Configuration

To display the following form, go to the Switch Ports Configuration form. Select a Switch Port number.



Switch Port 1 Configuration

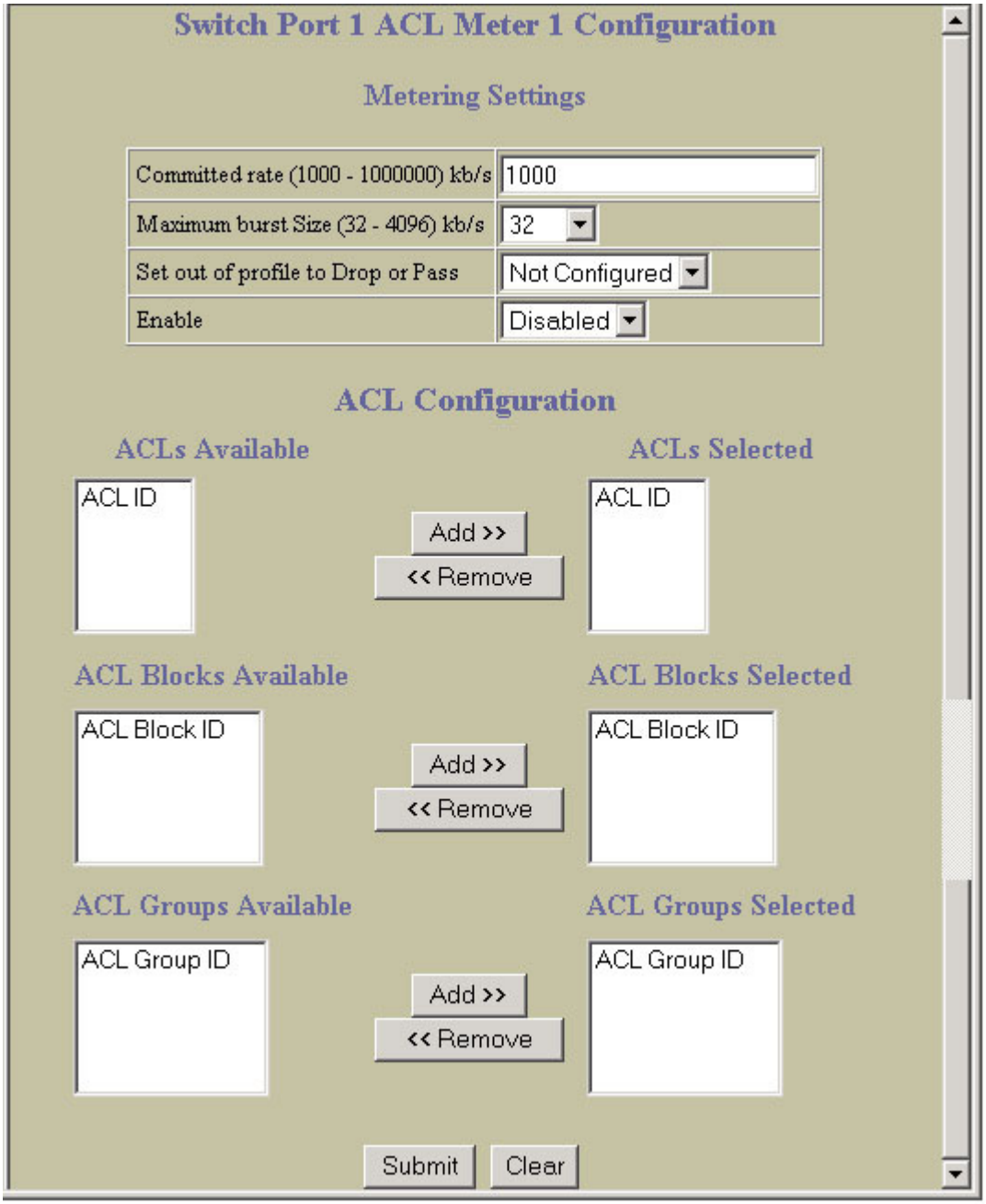
ACL Meter Configuration Table

ACL Meter	CIR	Max Burst	Drop/Pass	Enabled
1	1000	32	None	Disabled
2	1000	32	None	Disabled
3	1000	32	None	Disabled
4	1000	32	None	Disabled
5	1000	32	None	Disabled
6	1000	32	None	Disabled
7	1000	32	None	Disabled
8	1000	32	None	Disabled
9	1000	32	None	Disabled
10	1000	32	None	Disabled
11	1000	32	None	Disabled
12	1000	32	None	Disabled

This form summarizes the ACL meters parameters for individual switch ports.

Switch Port ACL Meter Configuration

To display the following form, go to the Switch Port Configuration form. Select an ACL meter number.



The following table describes the Switch Port ACL Meter Configuration controls:

Table 101 Switch Port ACL Meter Configuration controls

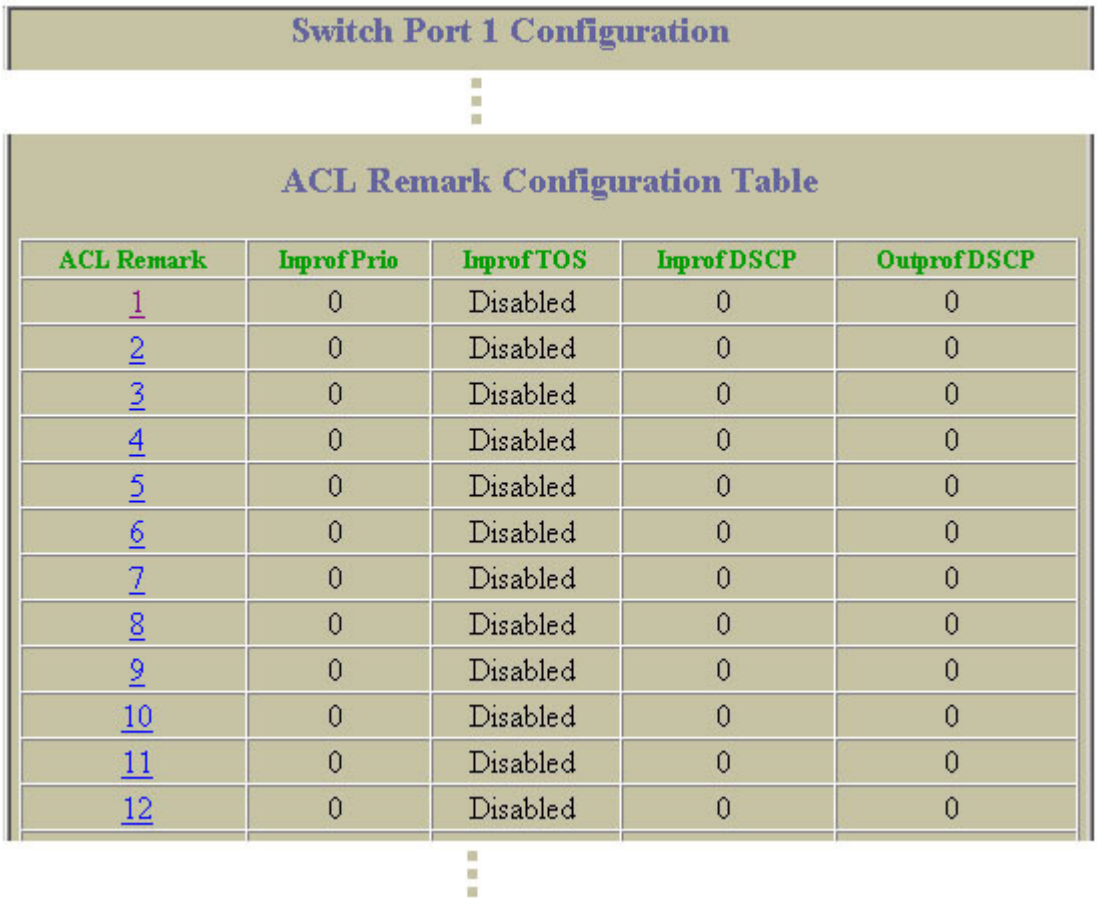
Control	Description
Committed rate (1000-1000000 kb/s)	Configures the committed rate, in Kilobits per second. The committed rate must be a multiple of 64.
Maximum burst Size (32-4096 kb/s)	Configures the maximum burst size, in Kilobits. Enter one of the following values for `mbsize`: 32, 64, 128, 256, 512, 1024, 2048, 4096
Set out of profile to Drop or Pass	Configures the ACL Meter to either drop or pass out-of-profile traffic.
Enable	Enables or disables the ACL meter.
ACLs Available	Lists the ACLs that you can add to the meter.

Table 101 Switch Port ACL Meter Configuration controls

Control	Description
ACLs Selected	Lists the ACLs associated with the meter. Select an ACL number in the ACLs Available list, and click **Add** to add the ACL to the meter. Select an ACL number in the ACLs Selected list, and click **Remove** to remove the ACL from the meter.
ACL Blocks Available	Lists the ACL Blocks that you can add to the meter.
ACL Blocks Selected	Lists the ACL Blocks associated with the meter. Select an ACL Block number in the ACL Blocks Available list, and click **Add** to add the ACL Block to the meter. Select an ACL Block number in the ACL Blocks Selected list, and click **Remove** to remove the ACL Block from the meter.
ACL Groups Available	Lists the ACL Groups that you can add to the meter.
ACL Groups Selected	Lists the ACL Groups associated with the meter. Select an ACL Group number in the ACL Groups Available list, and click **Add** to add the ACL Group to the meter. Select an ACL Group number in the ACL Groups Selected list, and click **Remove** to remove the ACL Group from the meter.

Switch Port ACL Remark Configuration

To display the following form, go to the Switch Ports Configuration form. Select a Switch Port number.



Switch Port 1 Configuration

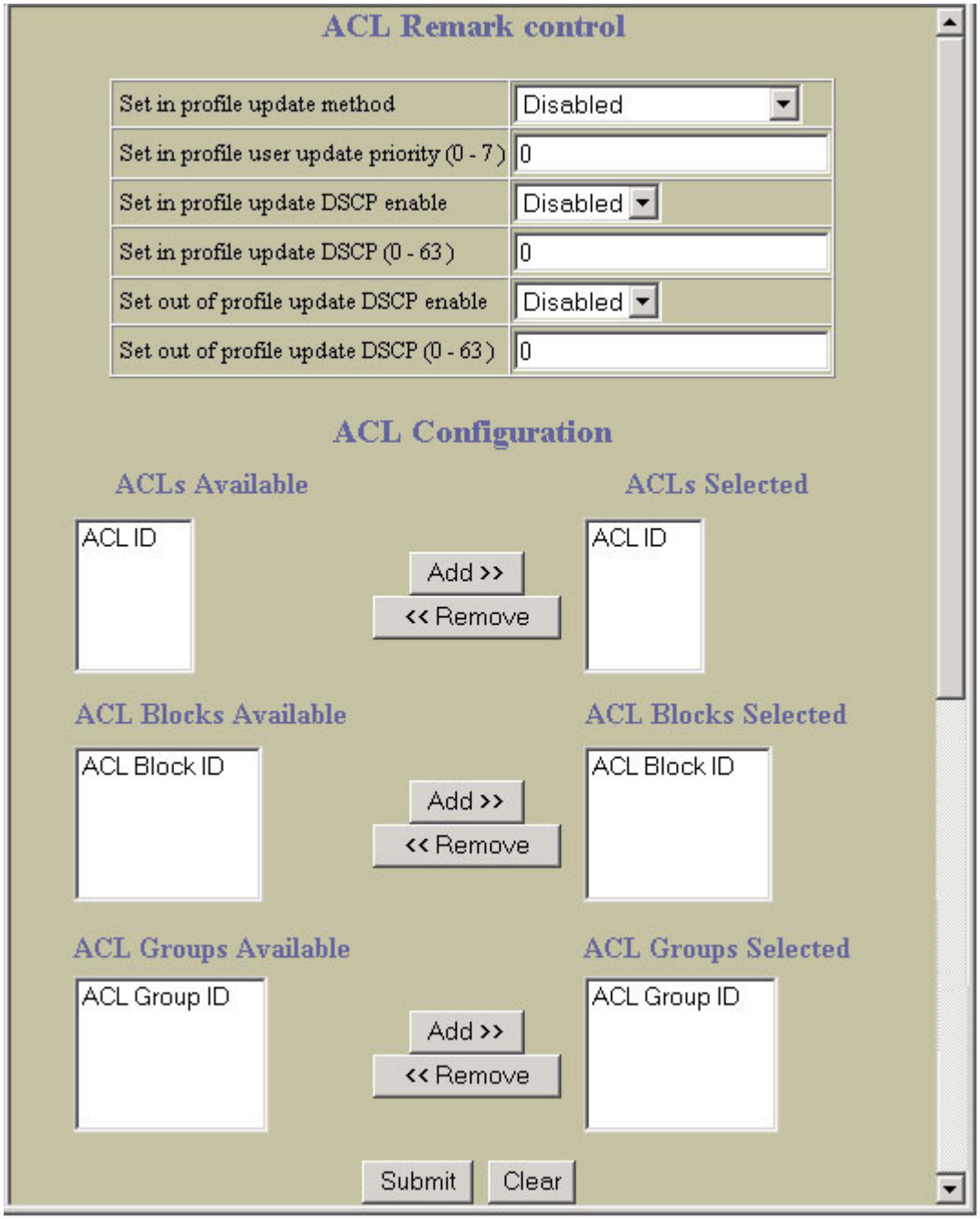
ACL Remark Configuration Table

ACL Remark	InprofPrio	InprofTOS	InprofDSCP	OutprofDSCP
1	0	Disabled	0	0
2	0	Disabled	0	0
3	0	Disabled	0	0
4	0	Disabled	0	0
5	0	Disabled	0	0
6	0	Disabled	0	0
7	0	Disabled	0	0
8	0	Disabled	0	0
9	0	Disabled	0	0
10	0	Disabled	0	0
11	0	Disabled	0	0
12	0	Disabled	0	0

This form summarizes the remark parameters for individual switch ports.

Switch Port Remark Configuration

To display the following form, go to the Switch Port Configuration form. Select an ACL remark number.



The following table describes the Switch Port Remark Configuration controls:

Table 102 Switch Port Remark Configuration controls

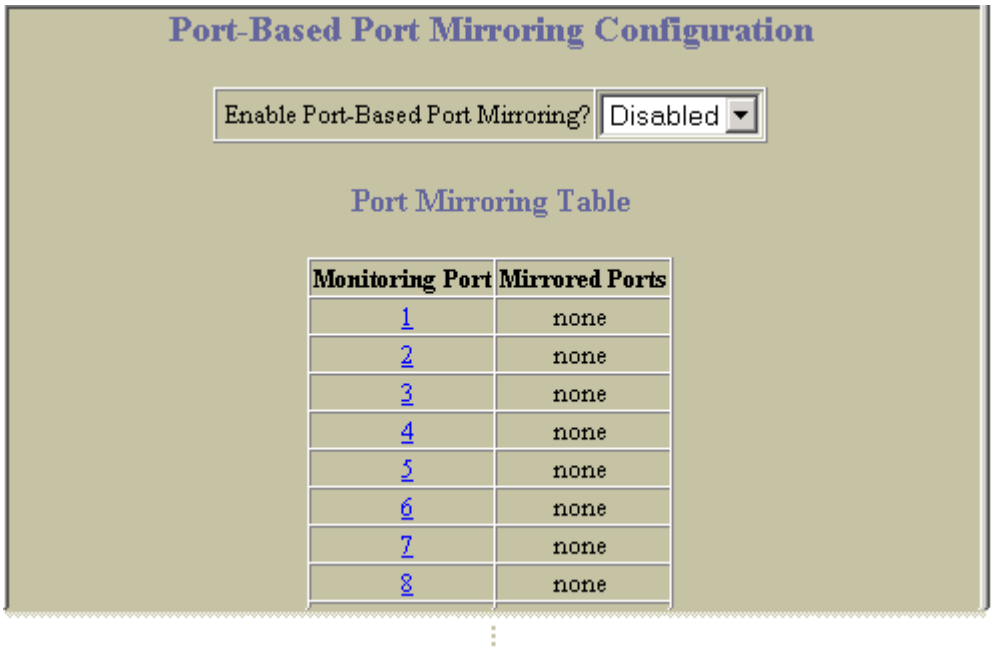
Control	Description
Set in profile update method	Defines the method used to update 802.1p priority updates, as follows: • User defined – Sets the 802.1p priority for In-Profile packets based on the configured value. • Use TOS precedence – Maps the TOS (Type of Service) priority to 802.1p priority for In-Profile packets. • Disabled – Disables 802.1p priority mapping for In-Profile packets.
Set in profile user update priority	Defines 802.1p value. The value is the priority bits information in the packet structure.
Set in profile update DSCP enable	Enables or disables DSCP updates for In-Profile packets.

Table 102 Switch Port Remark Configuration controls

Control	Description
Set in profile update DSCP (0-63)	Sets the DiffServ Code Point (DSCP) of In-Profile packets to the selected value.
Set out of profile update DSCP enable	Enables or disables DSCP updates for Out-of-Profile packets.
Set out of profile update DSCP (0-63)	Sets the DiffServ Code Point (DSCP) of Out-of-Profile packets to the selected value.
ACLs Available	Lists the ACLs that you can add to this remark process.
ACLs Selected	Lists the ACLs associated with this remark process. Select an ACL number in the ACLs Available list, and click **Add** to add the ACL to this remark process. Select an ACL number in the ACLs Selected list, and click **Remove** to remove the ACL from this remark process.
ACL Blocks Available	Lists the ACL Blocks that you can add to this remark process.
ACL Blocks Selected	Lists the ACL Blocks associated with this remark process. Select an ACL Block number in the ACL Blocks Available list, and click **Add** to add the ACL Block to this remark process. Select an ACL Block number in the ACL Blocks Selected list, and click **Remove** to remove the ACL Block from this remark process.
ACL Groups Available	Lists the ACL Groups that you can add to this remark process.
ACL Groups Selected	Lists the ACL Groups associated with this remark process. Select an ACL Group number in the ACL Groups Available list, and click **Add** to add the ACL Group to this remark process. Select an ACL Group number in the ACL Groups Selected list, and click **Remove** to remove the ACL Group from this remark process.

Port-Based Port Mirroring Configuration

To display the following form, select **Port-Based Port Mirroring** (click the underlined text, not the folder).



This form is used to configure, enable, and disable the Monitoring Port. When enabled, network packets being sent and/or received on a target port are duplicated and sent to a monitor port. By attaching a network analyzer to the monitor port, you can collect detailed information about your network performance and usage.

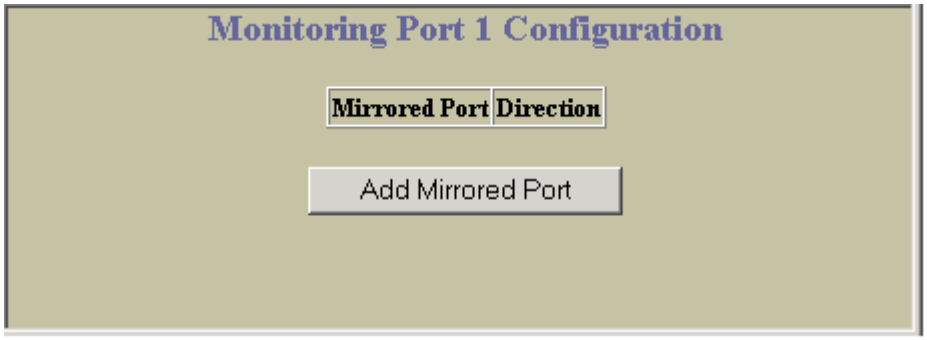
The following table describes the Port-Based Port Mirroring Configuration controls:

Table 103 Port Mirroring controls

Control	Description
Enable Port-Based Port Mirroring?	Enables or disables port mirroring on the switch. Port mirroring is disabled by default.
Monitoring Port	Selects a port number to configure the port as a monitoring port.
Mirrored Ports	Displays the port(s) currently mirrored for each monitoring port.

Monitoring Port Configuration

To display the following form, go to the Port-Based Port Mirroring Configuration form. Select a Monitoring Port number.



This form lists all mirrored ports for the selected port number.

Port Mirroring Configuration for Port

To display the following form, go to the Monitoring Port *x* Configuration form. Select a Mirrored Port number, or click **Add Mirrored Port**.

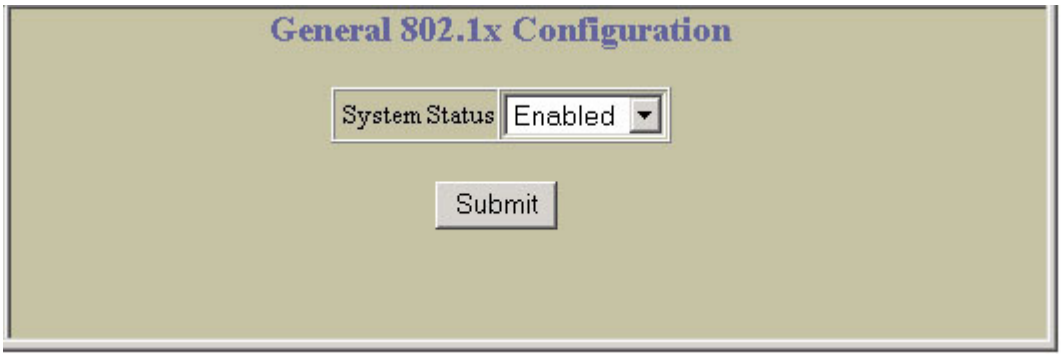
The following table describes the Port Mirroring Configuration for Port controls:

Table 104 Port Mirroring Configuration for Port controls

Control	Description
Mirrored Port	Adds the port to be mirrored.
Port Mirror Direction	Specifies the direction of the traffic, either **in** or **out**. It is necessary to specify the direction because: • If the source port of the frame matches the mirrored port and the mirrored direction is ingress or both (ingress and egress), the frame is sent to the mirrored port. • If the destination port of the frame matches the mirrored port and the mirrored direction is egress or both, the frame is sent to the monitoring port.

802.1x General Configuration

To display the following form, select **Layer 2 > 802.1x > General**.



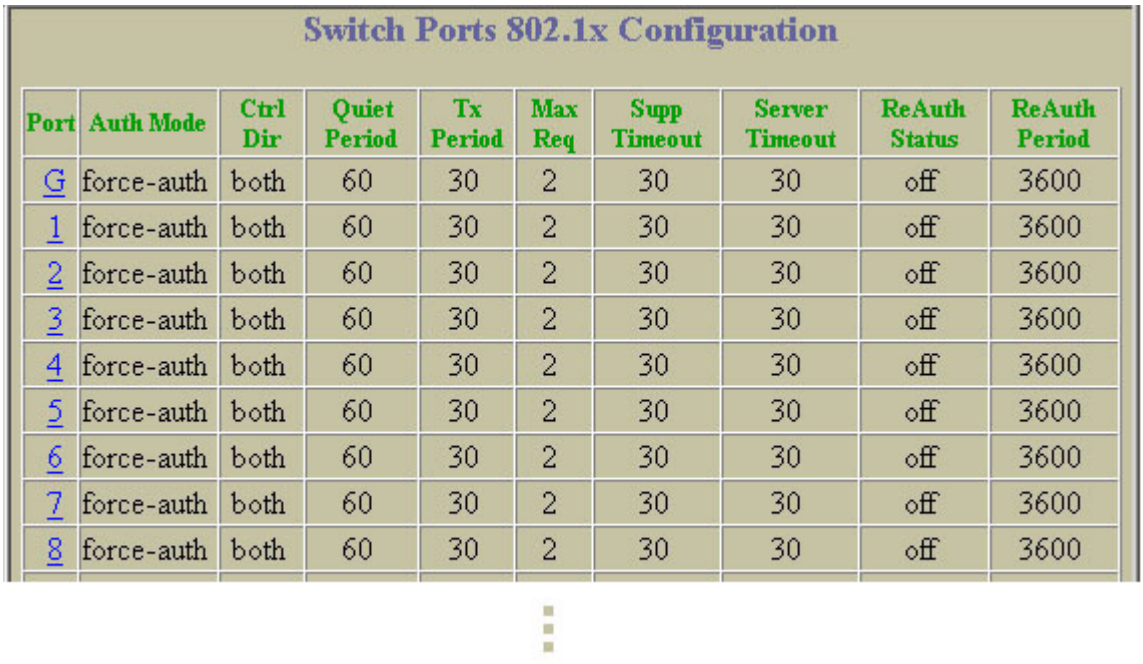
The following table describes the General 802.1x Configuration controls:

Table 105 General 802.1x Configuration controls

Control	Description
System Status	Enables or disables 802.1x Port-Based Network Access Control.

802.1x Switch Ports Configuration

To display the following form, select **Layer 2 > 802.1x > Switch Ports**.

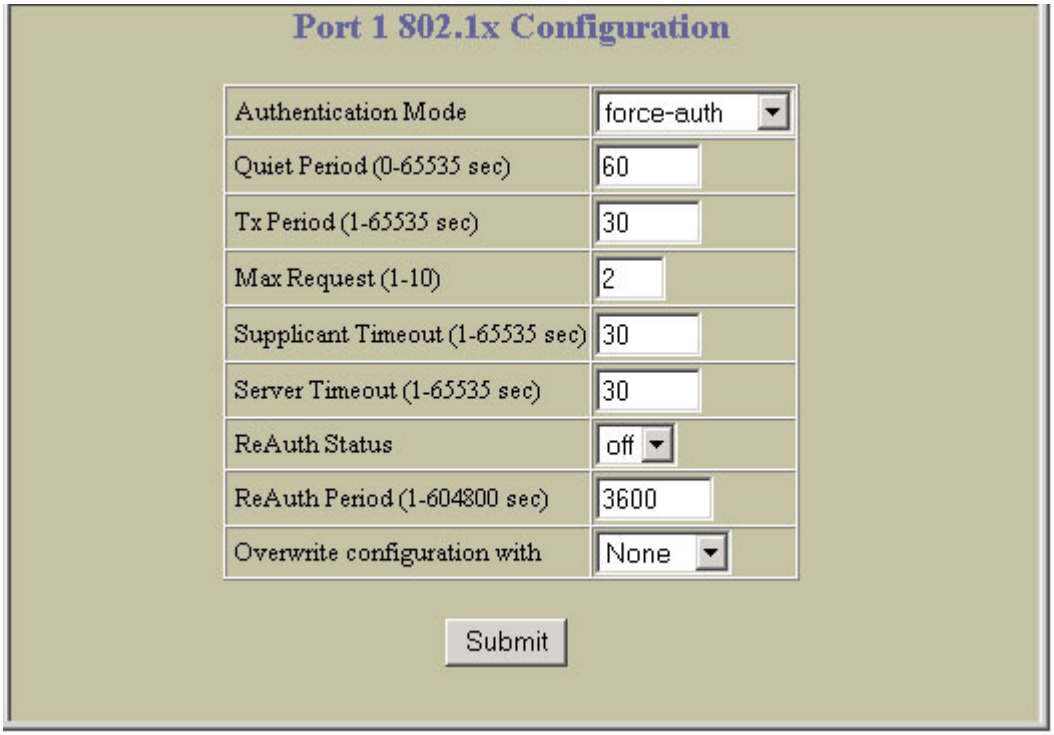


Port	Auth Mode	Ctrl Dir	Quiet Period	Tx Period	Max Req	Supp Timeout	Server Timeout	ReAuth Status	ReAuth Period
G	force-auth	both	60	30	2	30	30	off	3600
1	force-auth	both	60	30	2	30	30	off	3600
2	force-auth	both	60	30	2	30	30	off	3600
3	force-auth	both	60	30	2	30	30	off	3600
4	force-auth	both	60	30	2	30	30	off	3600
5	force-auth	both	60	30	2	30	30	off	3600
6	force-auth	both	60	30	2	30	30	off	3600
7	force-auth	both	60	30	2	30	30	off	3600
8	force-auth	both	60	30	2	30	30	off	3600

Select a port number to view the Switch Port 802.1x Configuration form.

802.1x Port Configuration

To display the following form, go to the Switch Ports 802.1x Configuration form. Select a port number.



The following table describes the Switch Ports 802.1x Configuration controls:

Table 106 Switch Ports 802.1x Configuration controls

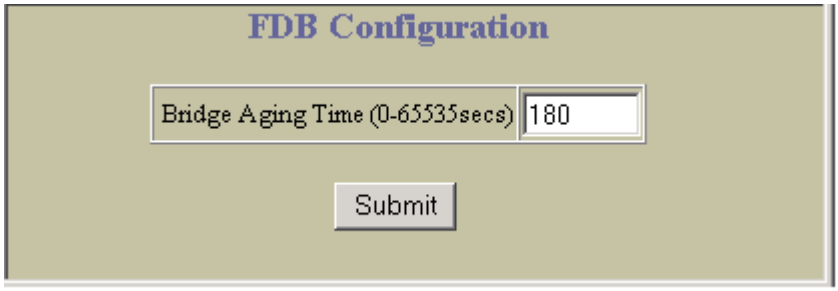
Control	Description
Auth Mode	Sets the type of access control for all ports: • **`force-unauth`**—the port is unauthorized unconditionally. • **`auto`**—the port is unauthorized until it is successfully authorized by the RADIUS server. • **`force-auth`**—the port is authorized unconditionally, allowing all traffic. The default value is **force-auth**.
Quiet Period (0-65535 sec)	Sets the time, in seconds, the authenticator waits before transmitting an EAP-Request/ Identity frame to the supplicant (client) after an authentication failure in the previous round of authentication. The default value is 60 seconds.
Tx Period (0-65535 sec)	Sets the time, in seconds, the authenticator waits for an EAP-Response/Identity frame from the supplicant (client) before retransmitting an EAP-Request/Identity frame. The default value is 30 seconds.
Max Req (1-10)	Sets the maximum number of times the authenticator retransmits an EAP-Request packet to the supplicant (client). The default value is 2.
Supplicant Timeout (0-65535 sec)	Sets the time, in seconds, the authenticator waits for an EAP-Response packet from the supplicant (client) before retransmitting the EAP-Request packet to the authentication server. The default value is 30 seconds.
Server Timeout (0-65535 sec)	Sets the time, in seconds, the authenticator waits for a response from the Radius server before declaring an authentication timeout. The default value is 30 seconds. The time interval between transmissions of the RADIUS Access-Request packet containing the supplicant's (client's) EAP-Response packet is determined by the current setting of `/cfg/sys/radius/timeout` (default is 3 seconds).
ReAuth Status	Sets the re-authentication status to `on` or `off`. The default value is `off`.
ReAuth Period (1-604800 sec)	Sets the time, in seconds, the authenticator waits before re-authenticating a supplicant (client) when periodic re-authentication is enabled. The default value is 3600 seconds.

Table 106 Switch Ports 802.1x Configuration controls

Control	Description
Overwrite Configuration with	Overwrites the port configuration settings with the global or default 802.1x settings.

FDB Configuration

To display the following form, select **Layer 2 > FDB**.



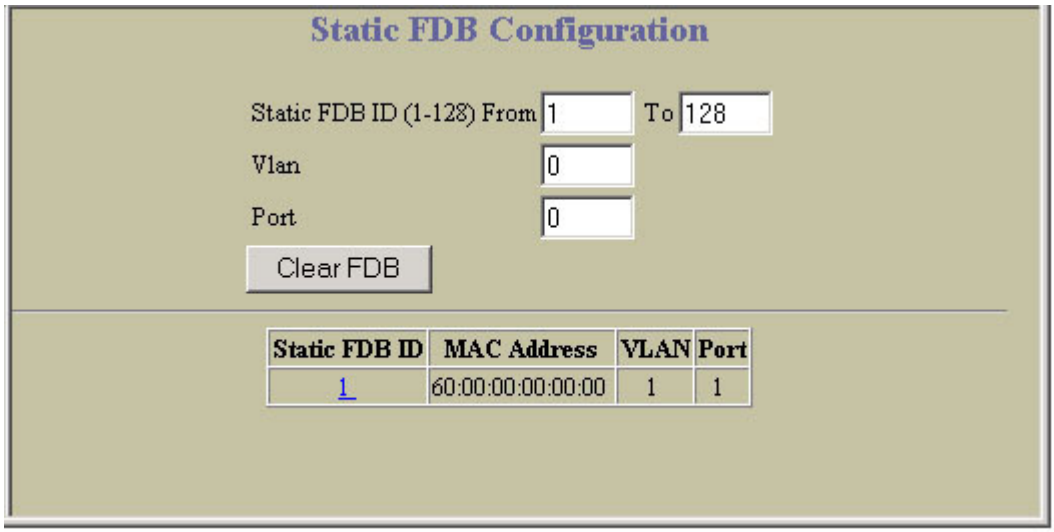
The following table describes the FDB Configuration controls:

Table 107 FDB Configuration controls

Control	Description
Bridge Aging Time (0-65535)	Configures the forwarding database aging time. The aging time specifies the amount of time the STP bridge waits without receiving a packet from a station before removing the station from the forwarding database. The default is 180 seconds. To disable aging, set this parameter to 0.

Static FDB Configuration

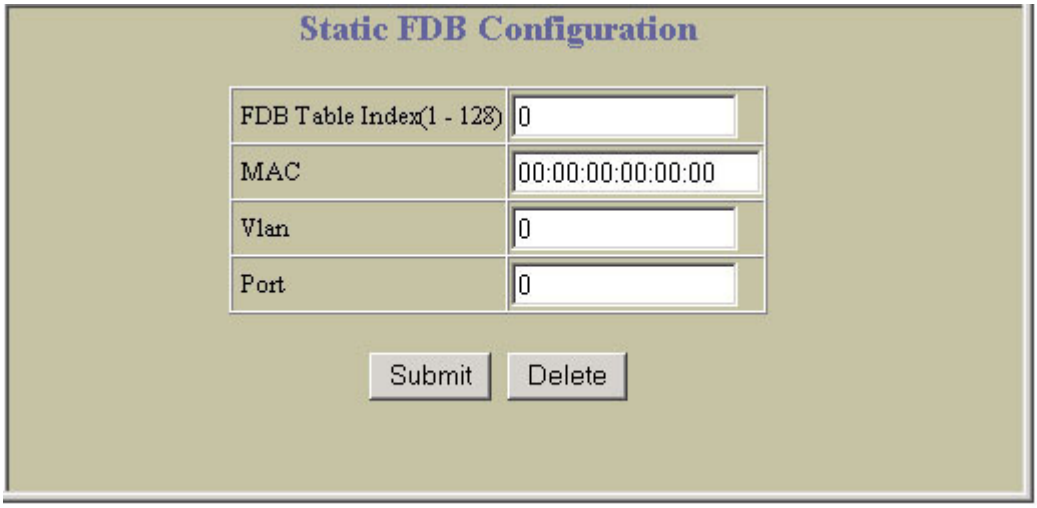
To display the following form, select **Layer 2 > FDB >Static FDB** (click the underlined text, not the folder).



This form summarizes the Static Forwarding Database entries. Select a static FDB ID number to display the Static FDB Configuration form. Click **Clear** to clear the static FDB entries.

Static FDB Configuration

To display the following form, select **Layer 2 > FDB >Static FDB > Add static FDB entry**.



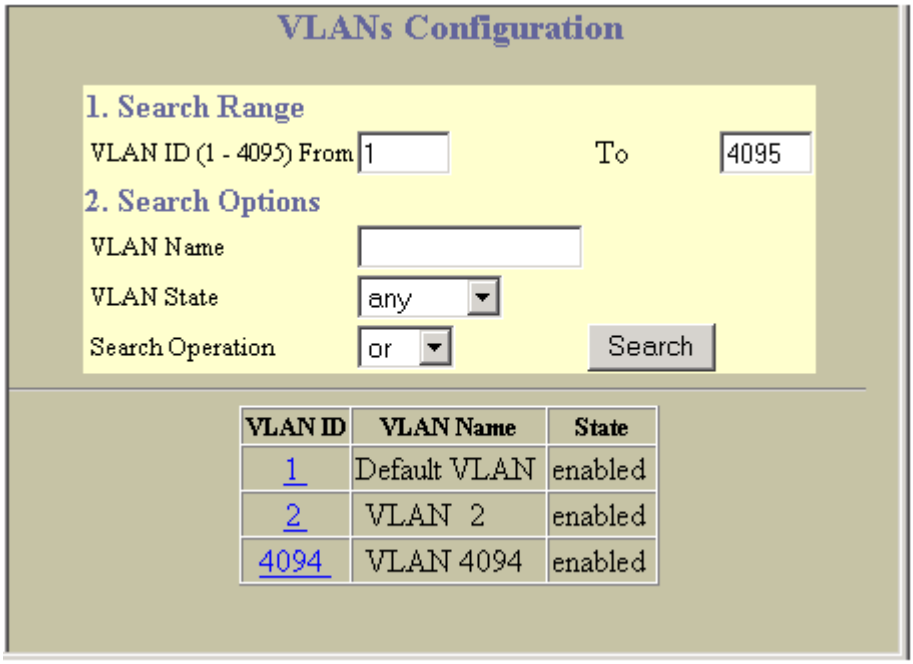
The following table describes the Static FDB Configuration controls:

Table 108 Static FDB Configuration controls

Control	Description
FDB Table Index (1-128)	Configures the index ID number of the static FDB entry.
MAC	Configures the MAC address of the static FDB entry.
Vlan	Configures the VLAN for the static FDB entry.
Port	Configures the port for the static FDB entry.

VLANs Configuration

To display the following form, select **Layer 2 > Virtual LANs** (click the underlined text, not the folder).



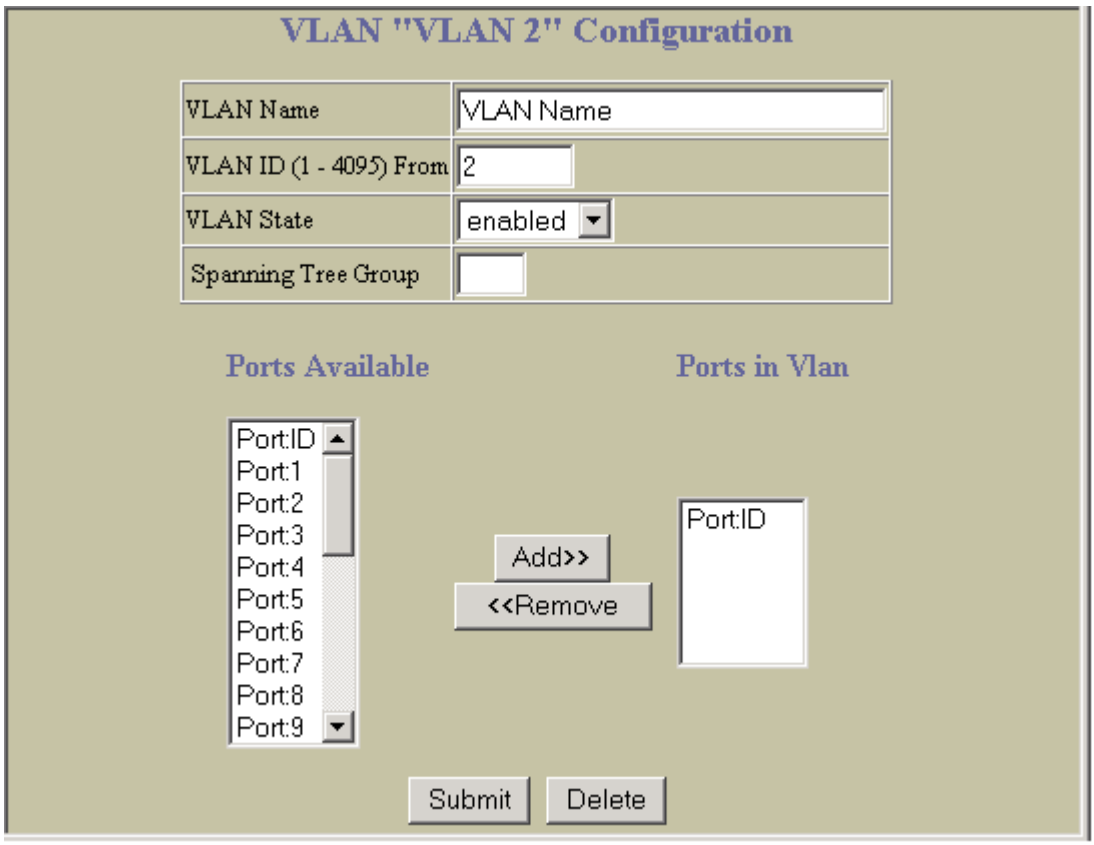
The following table describes the VLANs Configuration controls:

Table 109 VLANs Configuration controls

Control	Description
Search Range	To search for a VLAN, enter a range of VLAN numbers in the **From** and **To** fields.
Search Options	To focus the search for a VLAN, enter optional search parameters: • VLAN Name • VLAN State Fields that have a value of "any" are ignored during the search. Choose a search operation: • **or**: Search for VLANs specified in the search range that meet any of the criteria entered. • **and**: Search for VLANs specified in the search range that meet all of the criteria entered. Click **Search** to display VLANs that fit the range and meet the criteria entered.

VLAN Configuration

To display the following form, go to the VLANs Configuration form. Select a VLAN ID, or open the Virtual LANs folder and click **Add VLAN**.



The commands on this form configure VLAN attributes, change the status of the VLAN, delete the VLAN, and change the port membership of the VLAN. Up to 1,000 VLANs can be configured on the switch.

By default, the VLAN menu option is disabled except VLAN 1, which is enabled all the time.

The following table describes the VLAN Configuration controls:

Table 110 VLAN Configuration controls

Control	Description
VLAN Name	Assigns a name to the VLAN or changes the existing name. The default VLAN name is the first one.
VLAN ID (1-4095)	Assigns a numeric identifier to the VLAN.
VLAN State	Enables or disables the VLAN.

Table 110 VLAN Configuration controls

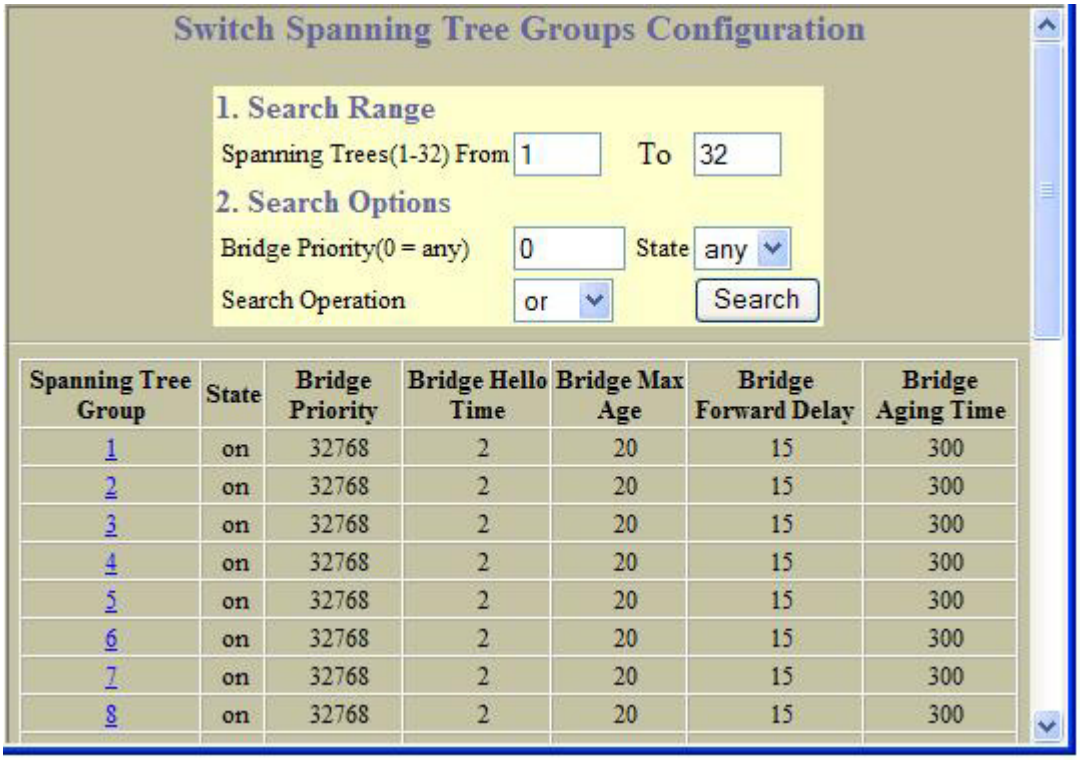
Control	Description
Spanning Tree Group	Assigns a VLAN to a Spanning Tree Group.
Ports Available	Lists the ports that can be added to the VLAN.
Ports in Vlan	Lists the ports that are members of the VLAN. Select a port number in the Ports Available list and click **Add** to add the port to the VLAN. Select a port number in the Ports in VLAN list and click **Remove** to remove the port from the VLAN.

NOTE: Each port must belong to at least one VLAN. Any port which is removed from a VLAN and which is not a member of any other VLAN is automatically added to default VLAN #1. You cannot remove a port from VLAN #1 if the port has no membership in any other VLAN.

Also, you cannot add a port to more than one VLAN unless the port has VLAN tagging turned on.

Switch Spanning Tree Groups Configuration

To display the following form, select **Layer 2 > Spanning Tree Groups** (click the underlined text, not the folder).



Spanning Tree Group	State	Bridge Priority	Bridge Hello Time	Bridge Max Age	Bridge Forward Delay	Bridge Aging Time
1	on	32768	2	20	15	300
2	on	32768	2	20	15	300
3	on	32768	2	20	15	300
4	on	32768	2	20	15	300
5	on	32768	2	20	15	300
6	on	32768	2	20	15	300
7	on	32768	2	20	15	300
8	on	32768	2	20	15	300

This form summarizes Spanning Tree Group parameters.

HP ProLiant BL p-Class GbE2 Interconnect Switch supports the IEEE 802.1d Spanning Tree Protocol (STP) and Per VLAN Spanning Tree (PVST+). STP is used to prevent loops in the network topology. Up to 32 Spanning Tree Groups can be configured on the switch.

NOTE: When RSTP is turned on, only STP group 1 can be configured.

The following table describes the Switch Spanning Tree Groups Configuration controls:

Table 111 Switch Spanning Tree Groups Configuration controls

Control	Description
Search Range	To search for a Spanning Tree Group, enter a range of group numbers in the **From** and **To** fields.
Search Options	To focus the search for a Spanning Tree Group, enter optional search parameters: • Bridge Priority • Spanning Tree State Fields that have a value of "any" are ignored during the search. Choose a search operation: • **or**: Search for Spanning Tree Groups specified in the search range that meet any of the criteria entered. • **and**: Search for Spanning Tree Groups specified in the search range that meet all of the criteria entered. Click **Search** to display Spanning Tree Groups that fit the range and meet the criteria entered.

Switch Spanning Tree Group Configuration

To display the following form, go to the Switch Spanning Tree Groups Configuration form. Select a Spanning Tree Group number, or open the Spanning Tree Groups folder and click **Add Spanning Tree Group**.

Spanning Tree bridge parameters can be configured for each Spanning Tree Group.

The following table describes the Switch Spanning Tree Group Configuration controls:

Table 112 Switch Spanning Tree Group Configuration controls

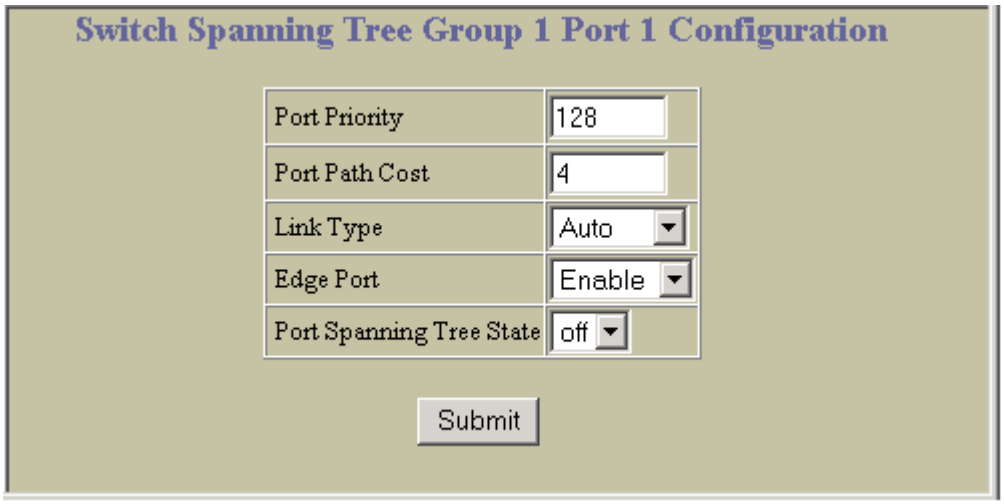
Control	Description
Spanning Tree Group ID (1-32)	Selects a Spanning Tree Group to configure.
Switch Spanning Tree State	Turns Spanning Tree **on** or **off** for the selected STP group.
Bridge Priority (0-65535)	Configures the bridge priority. The bridge priority parameter controls which bridge on the network is the STP root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. The range is 0 to 65535, and the default is 32768. **RSTP/MSTP**: The range is 0 to 61440, in steps of 4096 (0, 4096, 8192...), and the default is 32768. This command does not apply to MSTP. See the "Common Internal Spanning Tree Bridge Configuration" section for more information.
Bridge Hello Time (1-10 secs)	Configures the bridge hello time. The hello time specifies how often the root bridge transmits a configuration bridge protocol data unit (BPDU). Any bridge that is not the root bridge uses the root bridge hello value. The range is 1 to 10 seconds, and the default is 2 seconds. This command does not apply to MSTP. (See the "Common Internal Spanning Tree Bridge Configuration" section.)
Bridge Max Age (6-40 secs)	Configures the bridge maximum age. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the STP network. The range is 6 to 40 seconds, and the default is 20 seconds. This command does not apply to MSTP. See the "Common Internal Spanning Tree Bridge Configuration" section for more information.
Bridge Forward Delay (4-30 secs)	Configures the bridge forward delay parameter. The forward delay parameter specifies the amount of time that a bridge port has to wait before it changes from the listening state to the learning state and from the learning state to the forwarding state. The range is 4 to 30 seconds, and the default is 15 seconds. This command does not apply to MSTP. See the "Common Internal Spanning Tree Bridge Configuration" section for more information.
VLANs Available	Lists the VLANs that can be added to the Spanning Tree Group.
VLANs in STG	Lists the VLANs that are members of the Spanning Tree Group. Select a VLAN number in the VLANs Available list and click **Add** to add the VLAN to the Spanning Tree Group. Select a VLAN number in the VLANs in STG list and click **Remove** to remove the VLAN from the Spanning Tree Group.
Switch Spanning Tree Port Configuration Switch Port	Select a port number to display the switch spanning tree port configuration.

When configuring STP bridge parameters, the following formulas must be used:

- 2*(fwd-1) > mxage
- 2*(hello+1) < mxage

Switch Spanning Tree Group Port Configuration

To display the following form, go to the Switch Spanning Tree Group Configuration form. Select a Switch Port number.



Spanning Tree port parameters are used to modify STP operation on an individual port basis.

By default for STP/PVST+, Spanning Tree is turned Off for downlink ports (1-16), and turned On for uplink and cross-connect ports (17-24). By default for RSTP/MSTP, Spanning Tree is turned On for all ports, with downlink ports configured as Edge ports.

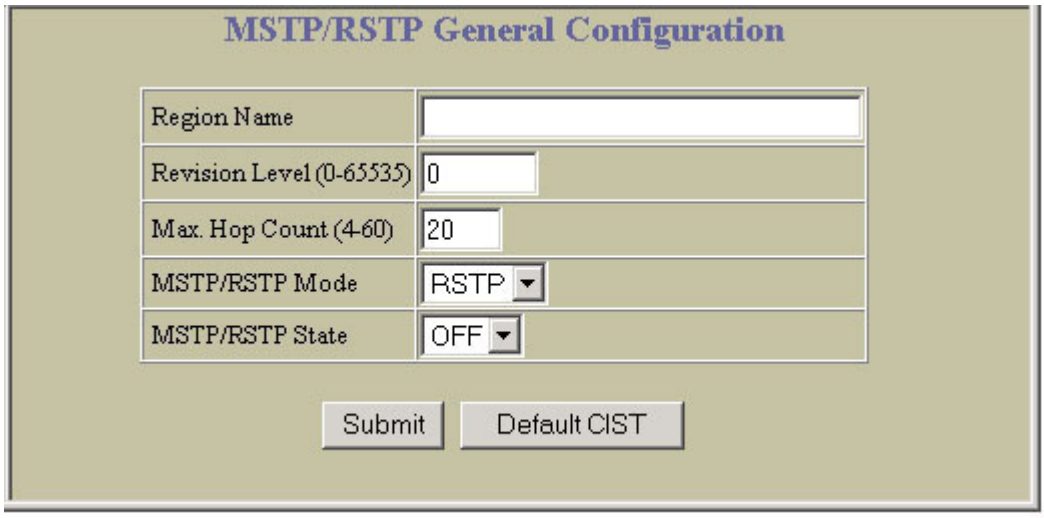
The following table describes the Switch Spanning Tree Group Port Configuration controls:

Table 113 Switch Spanning Tree Group Port Configuration controls

Control	Description
Port Priority	Configures the port priority. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. The range is 0 to 255, and the default is 128. **RSTP/MSTP**: The range is 0 to 240, in steps of 16 (0, 16, 32...) and the default is 128.
Port Path Cost	Configures the port path cost. The port path cost is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. The range is 1 to 65535. The default is 10 for 100Mbps ports, and 1 for Gigabit ports. A value of 0 indicates that the default cost will be computed for an auto-negotiated link speed. **RSTP/MSTP:** The range is 1 – 200000000, and the default it 20000 for Gigabit ports.
Link Type	Defines the type of link connected to the port, as follows: • **auto**: Configures the port to detect the link type, and automatically match its settings. • **p2p**: Configures the port for Point-To-Point protocol. • **shared**: Configures the port to connect to a shared medium (usually a hub). This command only applies when RSTP is turned on.
Edge Port	Enables or disables this port as an edge port. An edge port is not connected to a bridge, and can begin forwarding traffic as soon as the link is up. Configure server ports as edge ports (enabled). This command only applies when RSTP is turned on.
Port Spanning Tree State	Enables or disables STP on the port.

MSTP/RSTP General Configuration

To display the following form, select **Layer 2 > MSTP/RSTP > General.**



HP ProLiant BL p-Class GbE2 Interconnect Switch supports the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP). MSTP allows you to map many VLANs to a small number of spanning tree groups, each with its own topology.

Up to 32 spanning tree groups can be configured on the switch. MSTP/RSTP is turned off by default.

The following table describes the MSTP/RSTP General Configuration controls:

Table 114 MSTP/RSTP General Configuration controls

Control	Description
Region Name	Configures a name for the MSTP region. All devices within a MSTP region must have the same region name. The Region Name can have a maximum of 15 characters.
Revision Level (1-65535)	Configures a version number for the MSTP region. The version is used as a numerical identifier for the region. All devices within a MSTP region must have the same version number.
Max. Hop Count (4-60)	Configures the maximum number of bridge hops a packet may to traverse before it is dropped. The range is from 4 to 60 hops. The default is 20.
MSTP/RSTP Mode	Selects either Rapid Spanning Tree Protocol (RSTP) or Multiple Spanning Tree Protocol (MSTP). The default mode is RSTP.
MSTP/RSTP State	Globally turns RSTP/MSTP **on** or **off**. **Note:** When RSTP is turned on, the configuration parameters for STP group 1 apply to RSTP.
Default CIST	This button resets CIST general parameters to their default values.

NOTE:

- IEEE 802.1w standard-based RSTP implementation runs on one STG (i.e. same as one spanning tree instance) only. As a result, if 'rstp' mode is selected under the `/cfg/mrst/mode` command, then only a single RSTP instance (default for STG 1) is supported for all VLANs, including the Default VLAN 1.
- If multiple spanning tree instances are required, then select 'mstp' mode so that multiple VLANs are handled by multiple spanning tree instances, as specified by IEEE 802.1s standard-based MSTP implementation.
- Only IEEE 802.1s MSTP supports rapid convergence using IEEE 802.1w RSTP.
- PVST+ does not support rapid convergence in current versions.

NOTE:

The following configurations are **unsupported**:

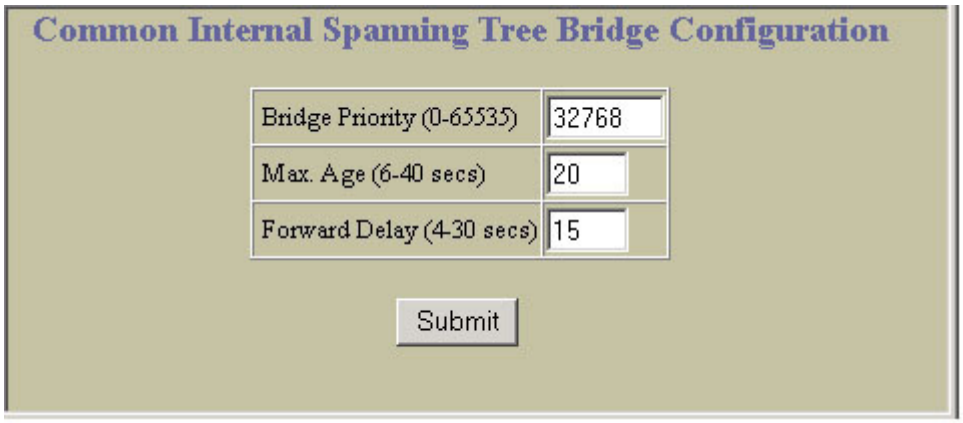
- HP PVST+ (default Spanning Tree setting) is NOT interoperable with Cisco Rapid PVST+.
- HP MSTP/RSTP (with mode set to either 'mstp' or 'rstp') is NOT interoperable with Cisco Rapid PVST+.

The following configurations are **supported**:

- HP PVST+ (default Spanning Tree setting) is interoperable with Cisco PVST+.
- HP MSTP/RSTP (with mode set to 'mstp') is interoperable with Cisco MST/RSTP.

Common Internal Spanning Tree Bridge Configuration

To display the following form, select **Layer 2 > MSTP/RSTP > CIST-Bridge**.



The CIST provides compatibility with different MSTP regions and with devices running different Spanning Tree instances. It is equivalent to Spanning Tree Group 0.

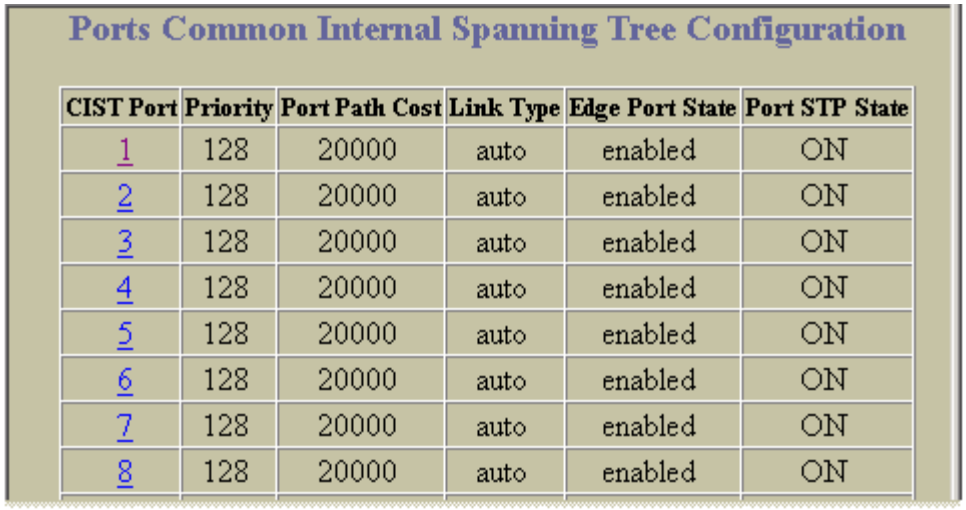
The following table describes the Common Internal Spanning Tree Bridge Configuration controls:

Table 115 Common Internal Spanning Tree Bridge Configuration controls

Control	Description
Bridge Priority (0-65535)	Configures the CIST bridge priority. The bridge priority parameter controls which bridge on the network is the MSTP root bridge. To make this switch the root bridge, configure the bridge priority lower than all other switches and bridges on your network. The lower the value, the higher the bridge priority. The range is 0 to 65535, and the default is 32768. This command does not apply to RSTP. See the "Switch Spanning Tree Group Configuration" section for more information.
Max. Age (6-40 secs)	Configures the CIST bridge maximum age. The maximum age parameter specifies the maximum time the bridge waits without receiving a configuration bridge protocol data unit before it reconfigures the MSTP network. The range is 6 to 40 seconds, and the default is 20 seconds. This command does not apply to RSTP. See the "Switch Spanning Tree Group Configuration" section for more information.
Forward Delay (4-30 secs)	Configures the CIST bridge forward delay parameter. The forward delay parameter specifies the amount of time that a bridge port has to wait before it changes from the listening state to the learning state and from the learning state to the forwarding state. The range is 4 to 30 seconds, and the default is 15 seconds. This command does not apply to RSTP. See the "Switch Spanning Tree Group Configuration" section for more information.

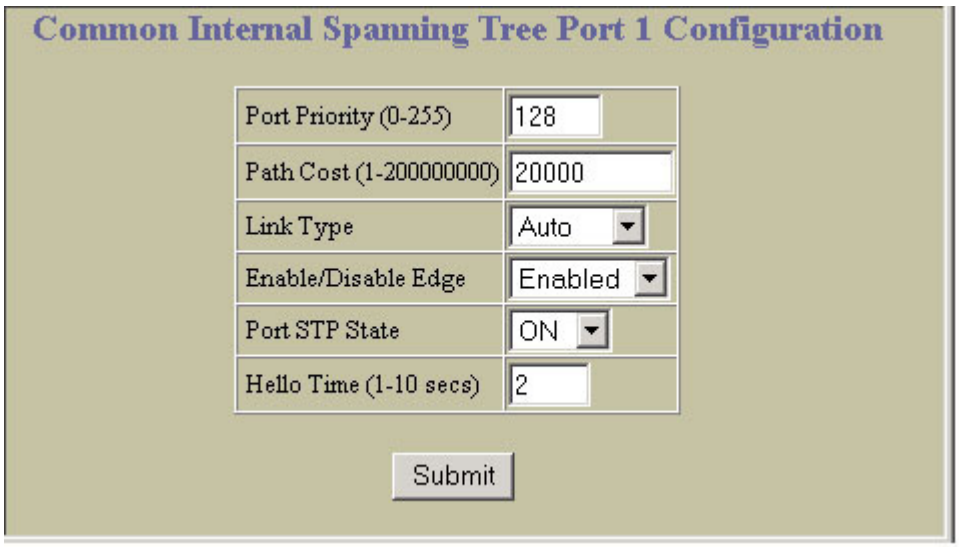
Ports Common Internal Spanning Tree Configuration

To display the following form, select **Layer 2 > MSTP/RSTP > CIST-Ports**.



Common Internal Spanning Tree Port Configuration

To display the following form, go to the Ports Common Internal Spanning Tree Configuration form. Select a CIST Port number.



This form summarizes the port CIST parameters. Common Internal Spanning Tree port parameters are used to modify MRST operation on an individual port basis. For each port, MSTP is turned on by default.

The following table describes the Common Internal Spanning Tree Port Configuration controls:

Table 116 Common Internal Spanning Tree Port Configuration controls

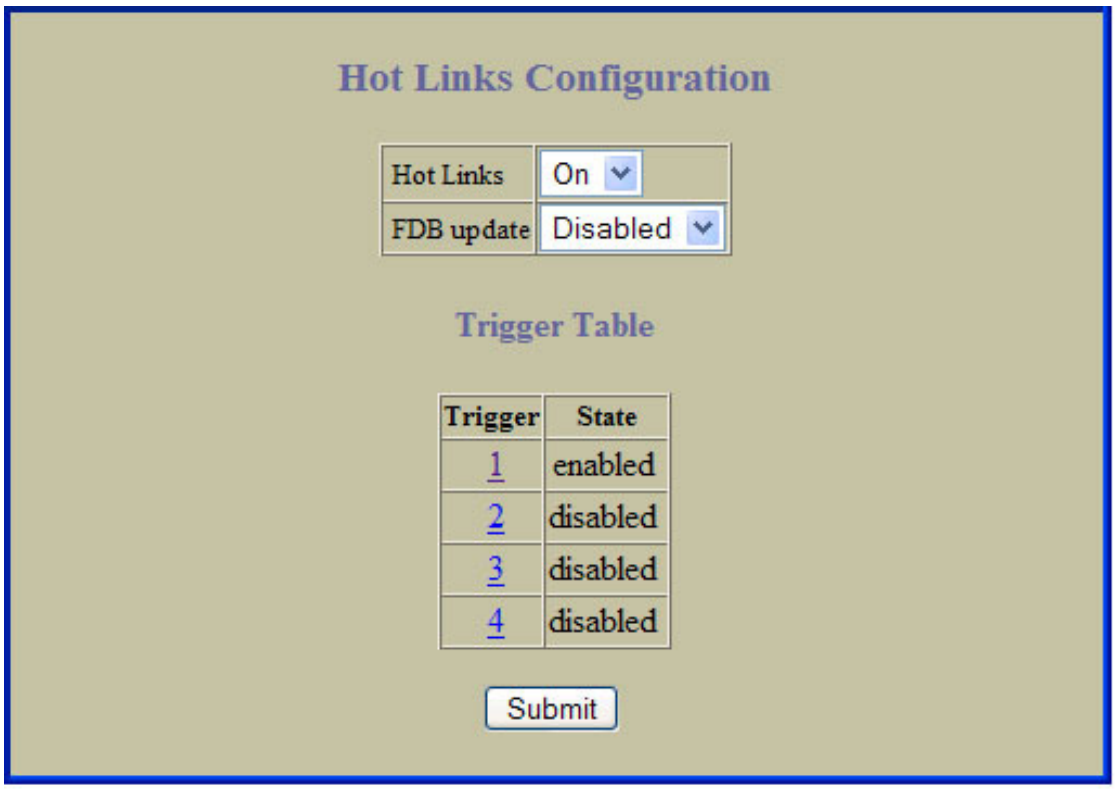
Control	Description
Port Priority (0-255)	Configures the CIST port priority. The port priority helps determine which bridge port becomes the designated port. In a network topology that has multiple bridge ports connected to a single segment, the port with the lowest port priority becomes the designated port for the segment. The range is 0 to 255, in steps of 16 (0, 16, 32...) and the default is 128.
Path Cost (1-200000000)	Configures the CIST port path cost. The port path cost is used to help determine the designated port for a segment. Generally speaking, the faster the port, the lower the path cost. The default is 20000 for Gigabit ports.

Table 116 Common Internal Spanning Tree Port Configuration controls

Control	Description
Link Type	Defines the type of link connected to the port, as follows: • **auto**: Configures the port to detect the link type, and automatically match its settings. • **p2p**: Configures the port for Point-To-Point protocol. • **shared**: Configures the port to connect to a shared medium (usually a hub). The default link type is **auto**.
Enable/Disable Edge	Enables or disables this port as an edge port. An edge port is not connected to a bridge, and can begin forwarding traffic as soon as the link is up. Configure server ports as edge ports (enabled). This command is disabled by default.
Port STP State	Turns MRST **on** or **off** for this port.
Hello Time (1-10 secs)	Configures how often "keep alive" BPDU messages are transmitted.

Hot Links Configuration

To display the following form, select **Layer 2 > Hot Links**.



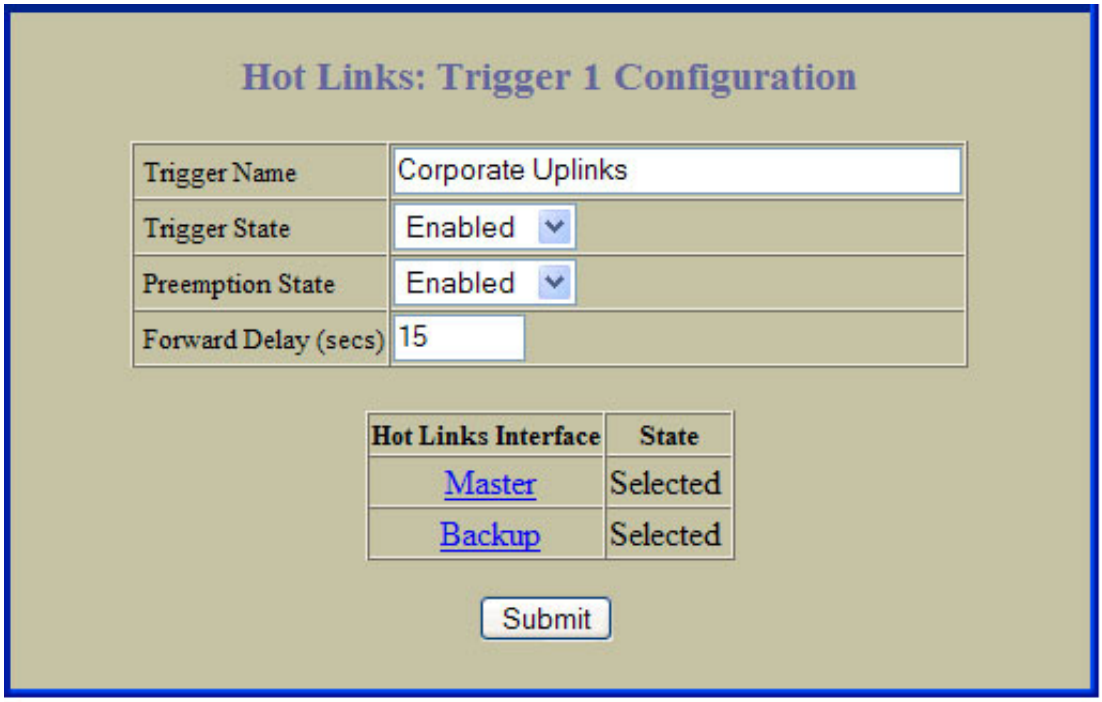
The following table describes the Hot Links Configuration controls:

Table 117 Hot Links Configuration controls

Control	Description
Hot Links	Globally turns Hot Links `on` or `off`.
FDB Update	Enables or disables FDB Update, which allows the GbE2 to send FDB and MAC update packets over the active interface. The default value is `disabled`.
Trigger	Selects a Hot Links trigger number.
State	Displays the operational state of each trigger.

Hot Links Trigger Configuration

To display the following form, go to the Hot Links Configuration form. Select a Trigger number.



The following table describes the Hot Links Trigger Configuration controls:

Table 118 Hot Links Trigger Configuration controls

Control	Description
Trigger Name	Configures a name for the trigger.
Trigger State	Enables or disables the Hot Links trigger.
Preemption State	Enables or disables pre-emption, which allows the Master interface to transition to the Active state whenever it becomes available. The default option is `enabled`.
Forward Delay	Configures the Forward Delay interval, in seconds. The default value is 1.
Hot Links Interface	Selects a Hot Links interface: Master or Backup
State	Displays the state of the Hot Links interface: Selected (contains port/trunk) or Empty

Hot Links Master Configuration

To display the following form, go to the Hot Links Trigger Configuration form. Select **Master**.

The following table describes the Hot Links Master Configuration controls:

Table 119 Hot Links Master Configuration controls

Control	Description
Port	Adds the selected port to the Master interface.
Trunk	Adds the selected trunk to the Master interface.

Hot Links Backup Configuration

To display the following form, go to the Hot Links Trigger Configuration form. Select **Backup**.

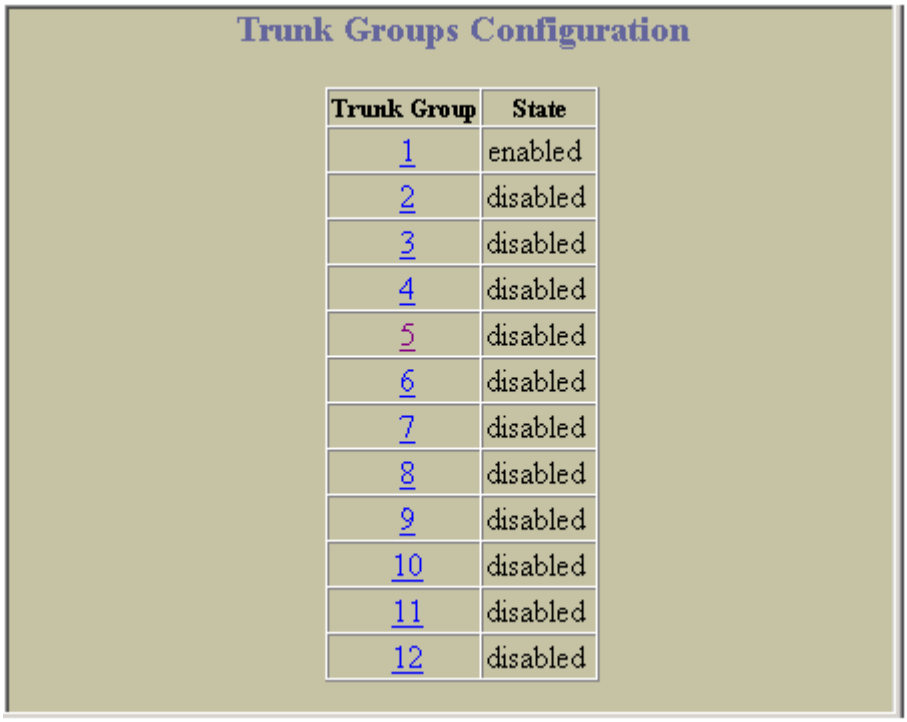
The following table describes the Hot Links Backup Configuration controls:

Table 120 Hot Links Backup Configuration controls

Control	Description
Port	Adds the selected port to the Backup interface.
Trunk	Adds the selected trunk to the Backup interface.

Trunk Groups Configuration

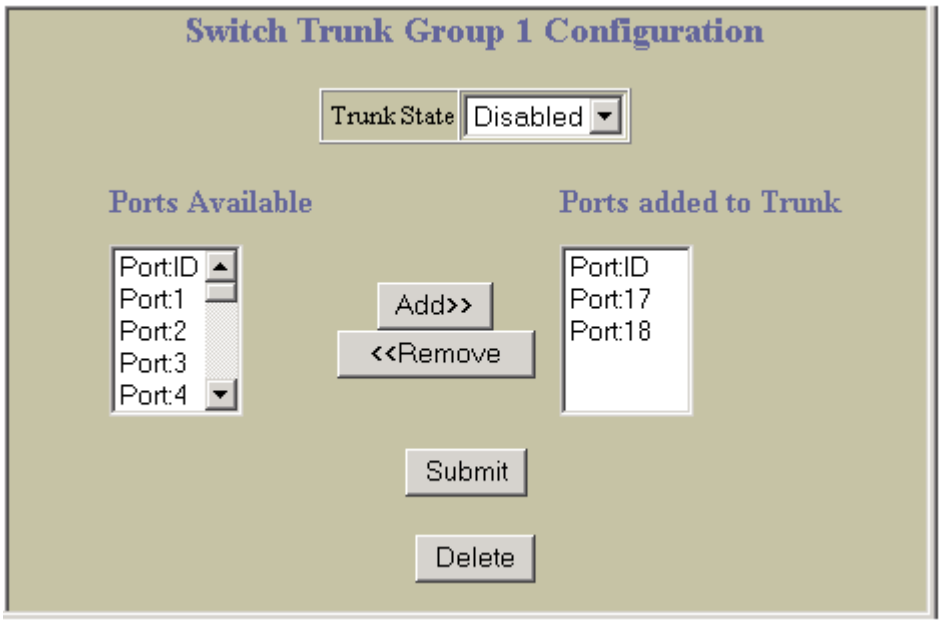
To display the following form, select **Layer 2 > Trunk Groups**.



This form provides a summary of the state of all trunk groups.

Switch Trunk Group Configuration

To display the following form, go to the Trunk Groups Configuration form. Select a Trunk Group number.



This form enables you to configure a selected switch trunk group.

Trunk groups can provide super-bandwidth connections between GbE2 Interconnect Switches or other trunk capable devices. A **trunk** is a group of ports that act together, combining their bandwidth to create a single, larger port. Up to 12 trunk groups can be configured on the GbE2 Interconnect Switch with the following restrictions:

- Any physical switch port can belong to no more than one trunk group.
- Up to six ports/trunks can belong to the same trunk group.

- All ports in a trunk must have the same configuration for speed, flow control, and autonegotiation.
- Trunking from other devices must comply with Cisco® EtherChannel® technology.
- By default, port 17 and 18 are trunked.

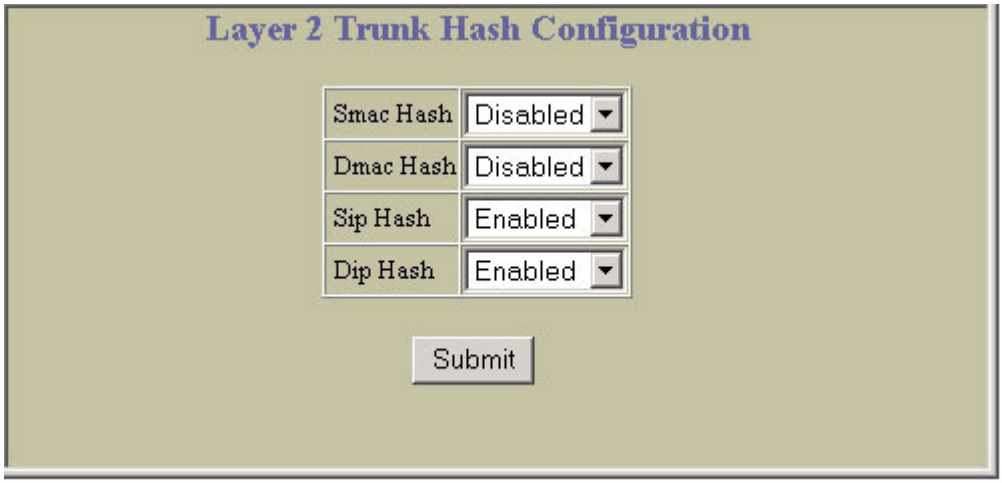
The following table describes the Switch Trunk Group Configuration controls:

Table 121 Switch Trunk Group Configuration controls

Control	Description
Trunk State	Enables or disables the Trunk Group.
Ports Available	Lists the ports that you can add to the Trunk Group.
Ports added to Trunk	Lists the ports that are members of the Trunk Group. Select a port number in the Ports Available list, and click **Add** to add the port to the Trunk Group. Select a port number in the Ports added to Trunk list, and click **Remove** to remove the port from the Trunk Group.

Trunk Hash Configuration

To display the following form, select **Layer 2 > Trunk Hash**.



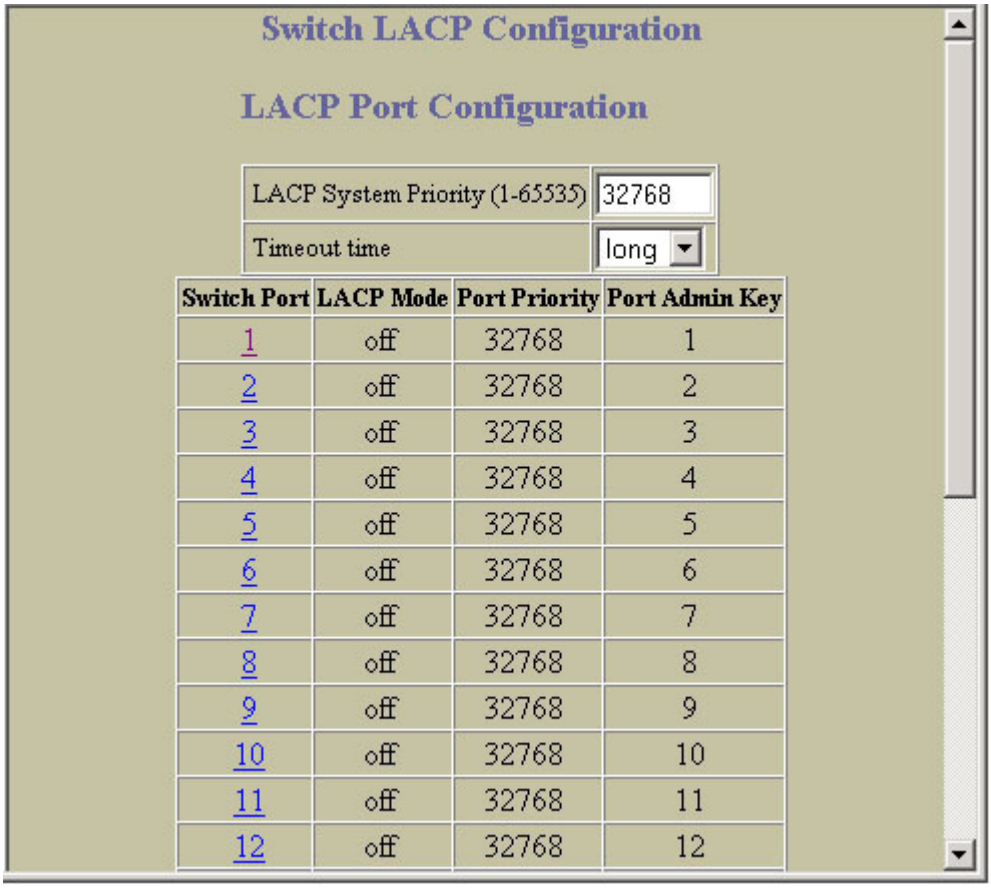
The following table describes the Layer 2 Trunk Hash Configuration controls:

Table 122 Layer 2 Trunk Hash Configuration controls

Control	Description
Smac	Enable or disable trunk hashing on the source MAC.
Dmac	Enable or disable trunk hashing on the destination MAC.
Sip	Enable or disable trunk hashing on the source IP.
Dip	Enable or disable trunk hashing on the destination IP.

LACP Configuration

To display the following form, select **Layer 2 > LACP**.



The following table describes the Switch LACP Configuration controls:

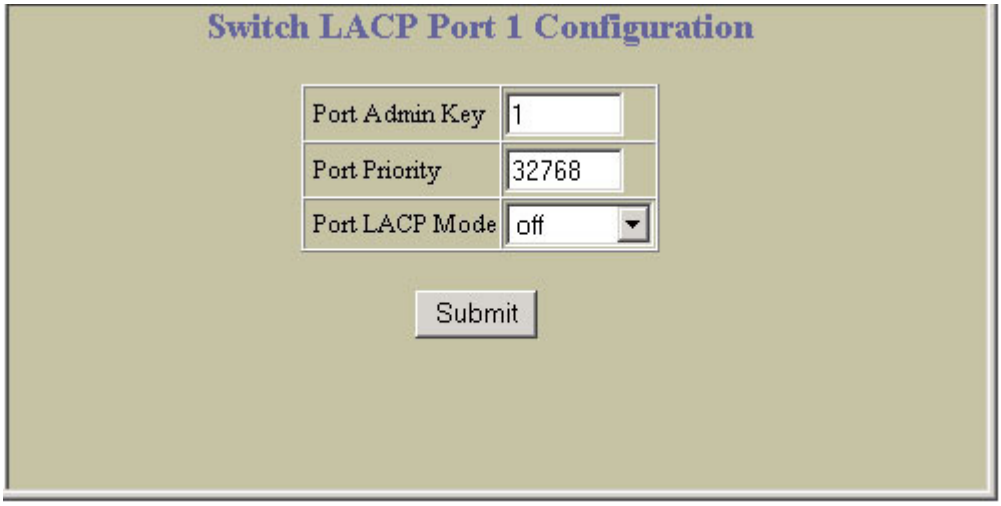
Table 123 Switch LACP Configuration controls

Control	Description
LACP System Priority (1-65535)	Defines the priority value (1 through 65535) for the switch. Lower numbers provide higher priority. The default value is 32768.
Timeout time	Defines the timeout period before invalidating LACP data from a remote partner. Choose **`short`** (3 seconds) or **`long`** (90 seconds). The default value is **`long`**.

NOTE: HP recommends that you use a timeout value of **`long`**, to reduce LACPDU processing. If your switch's CPU utilization rate remains at 100% for periods of 90 seconds or more, consider using static trunks instead of LACP.

LACP Port Configuration

To display the following form, go to the Switch LACP Configuration form. Select a port number.



The following table describes the LACP Port Configuration controls:

Table 124 LACP Port Configuration controls

Control	Description
Port Admin Key	Set the admin key for this port. Only ports with the same admin key and oper key (operational state generated internally) can form a LACP trunk group.
Port Priority	Sets the priority value for the selected port. Lower numbers provide higher priority. Default is 128.
Port LACP Mode	Set the LACP mode for this port, as follows: • **off**: Turn LACP off for this port. You can use this port to manually configure a static trunk. The default value is `off`. • **active:** Turn LACP on and set this port to active. Active ports initiate LACPDUs. • **passive:** Turn LACP on and set this port to passive. Passive ports do not initiate LACPDUs, but respond to LACPDUs from active ports.

Uplink Fast Configuration

To display the following form, select **Layer 2 > UpLink Fast**.

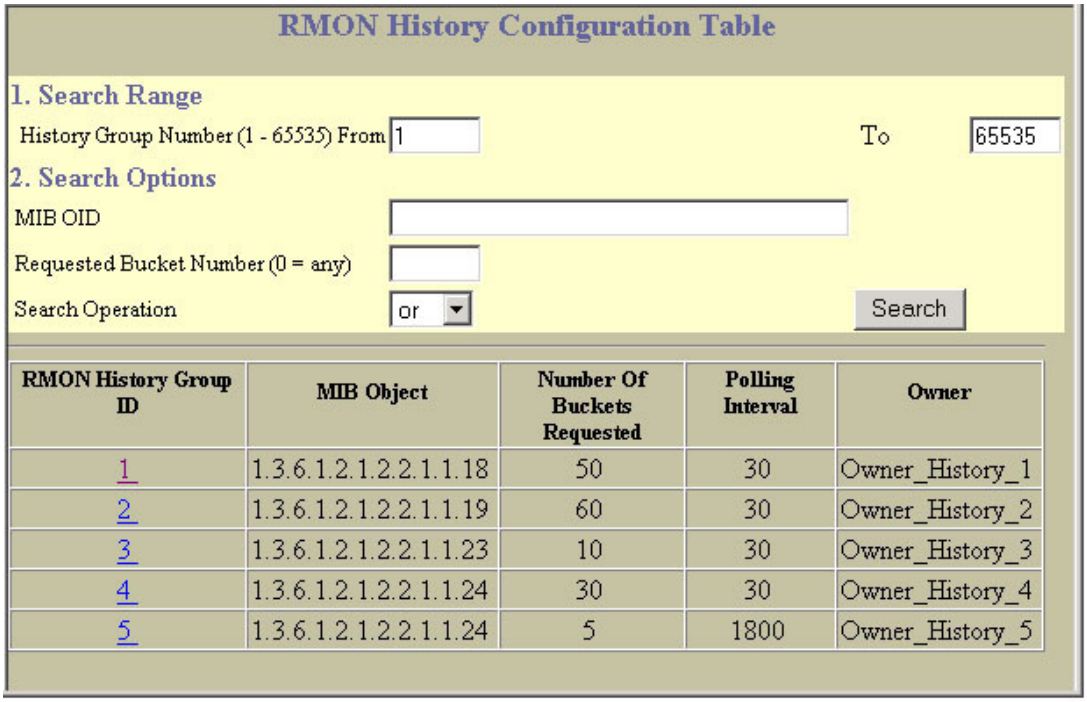
The following table describes the Uplink Fast Configuration controls:

Table 125 Uplink Fast Configuration controls

Control	Description
Enabled?	Enables or disables Fast Uplink Convergence, which provides rapid Spanning Tree convergence to an upstream switch during failover.
NOTE: When enabled, this feature increases bridge priorities to 65500 for all STGs and path cost by 3000 for all external STP ports.	
Update Rate (10-200)	Configures the station update rate. The default value is 40.

RMON History Configuration Table

To display the following form, select **RMON > History** (click the underlined text, not the folder).



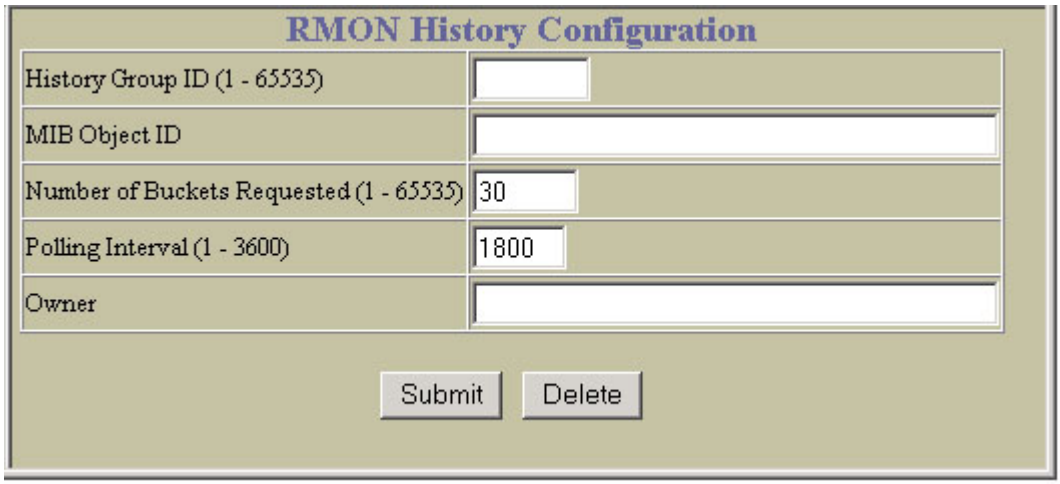
The following table describes the RMON History Groups Configuration controls:

Table 126 RMON History Configuration controls

Control	Description
Search Range	To search for a History Group, enter a range of numbers in the **From** and **To** fields.
Search Options	To focus the search for a History Group, enter optional search parameters: • MIB OID • Requested Number of Buckets Fields that have a value of "any" are ignored during the search. Choose a search operation: • **or**: Search for History Groups specified in the search range that meet any of the criteria entered. • **and**: Search for History Groups specified in the search range that meet all of the criteria entered. Click **Search** to display History Groups that fit the range and meet the criteria entered.

RMON History Configuration

To display the following form, go to the RMON History Groups Configuration form. Select a History Group, or open the History folder and click **Add History Group.**



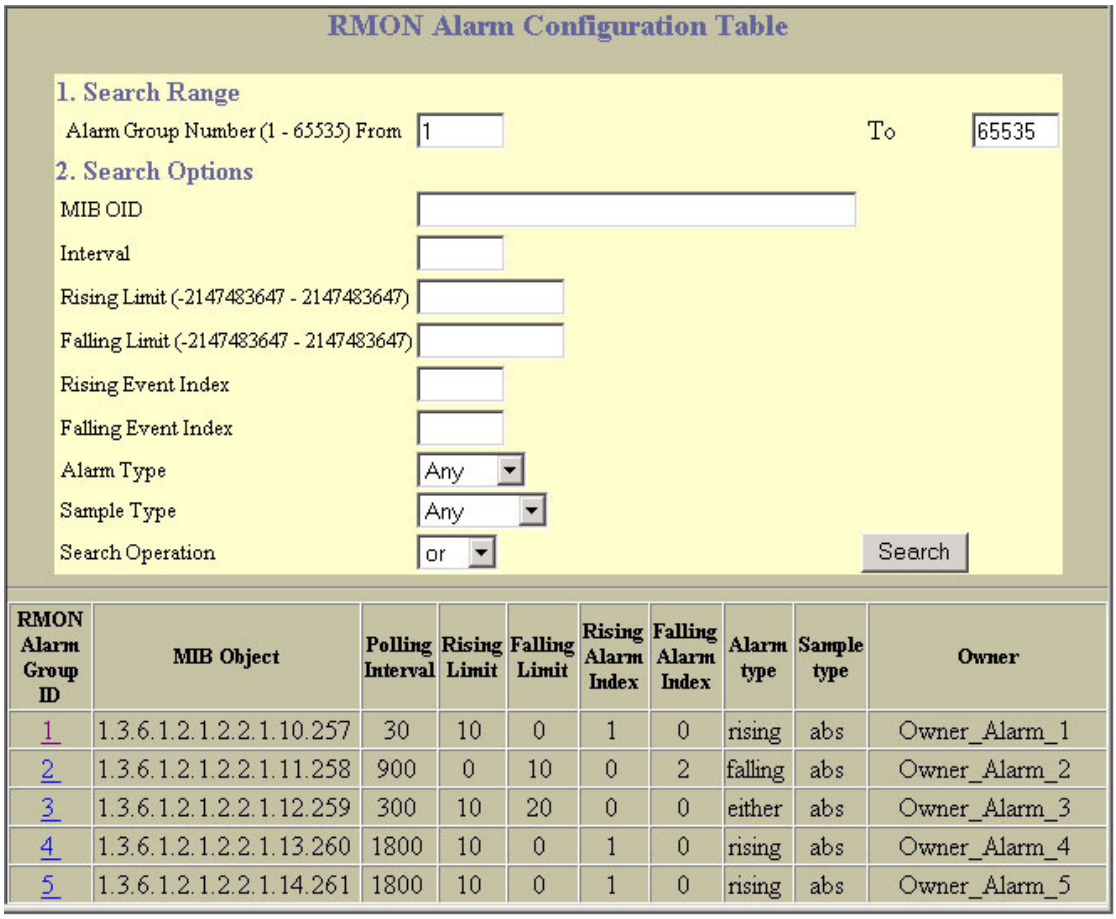
The following table describes the History Group Configuration controls:

Table 127 History Group Configuration controls

Control	Description
History Group ID (1-65535)	Configures a numeric identifier for the selected History index.
MIB Object ID	Configures the interface MIB Object Identifier. The interface OID can have a maximum of 127 characters.
Number of Buckets Requested (1-65535)	Configures the number of requested buckets, which is the number of data slots into which data is to be saved. The range is from 1 to 65535. The default is 30.
NOTE: The maximum number of buckets that can be granted is 50.	
Polling Interval (1-3600)	Configures the time interval over which the data is sampled for each bucket. The range is from 1 to 3600 seconds. The default value is 1800 seconds.
Owner	Enter a text string that identifies the person or entity that uses this History Group. The owner can have a maximum of 127 characters.

RMON Alarm Configuration Table

To display the following form, select **RMON > Alarm** (click the underlined text, not the folder).



RMON Alarm Group ID	MIB Object	Polling Interval	Rising Limit	Falling Limit	Rising Alarm Index	Falling Alarm Index	Alarm type	Sample type	Owner
1	1.3.6.1.2.1.2.2.1.10.257	30	10	0	1	0	rising	abs	Owner_Alarm_1
2	1.3.6.1.2.1.2.2.1.11.258	900	0	10	0	2	falling	abs	Owner_Alarm_2
3	1.3.6.1.2.1.2.2.1.12.259	300	10	20	0	0	either	abs	Owner_Alarm_3
4	1.3.6.1.2.1.2.2.1.13.260	1800	10	0	1	0	rising	abs	Owner_Alarm_4
5	1.3.6.1.2.1.2.2.1.14.261	1800	10	0	1	0	rising	abs	Owner_Alarm_5

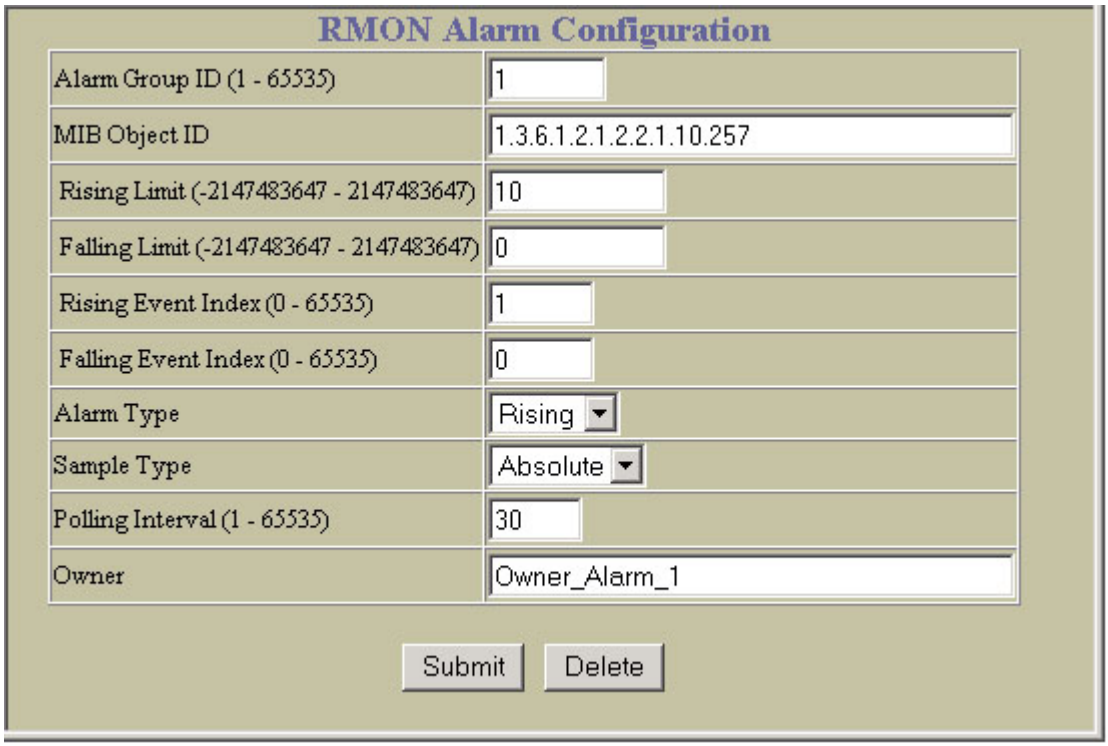
The following table describes the Alarm Groups Configuration controls:

Table 128 RMON Alarm Configuration controls

Control	Description
Search Range	To search for a RMON Alarm, enter a range of numbers in the **From** and **To** fields.
Search Options	To focus the search for a RMON Alarm, enter optional search parameters: • MIB OID • Interval • Rising Limit • Falling Limit • Rising Event Index • Falling Event Index • Alarm Type • Sample Type Fields that have a value of “any” are ignored during the search. Choose a search operation: • **or**: Search for Alarms specified in the search range that meet any of the criteria entered. • **and**: Search for Alarms specified in the search range that meet all of the criteria entered. Click **Search** to display RMON Alarms that fit the range and meet the criteria entered.

RMON Alarm Configuration

To display the following form, go to the RMON Alarm Groups Configuration form. Select an Alarm Group, or open the Alarm folder and click **Add Alarm Group.**



The following table describes the Alarm Group Configuration controls:

Table 129 Alarm Group Configuration controls

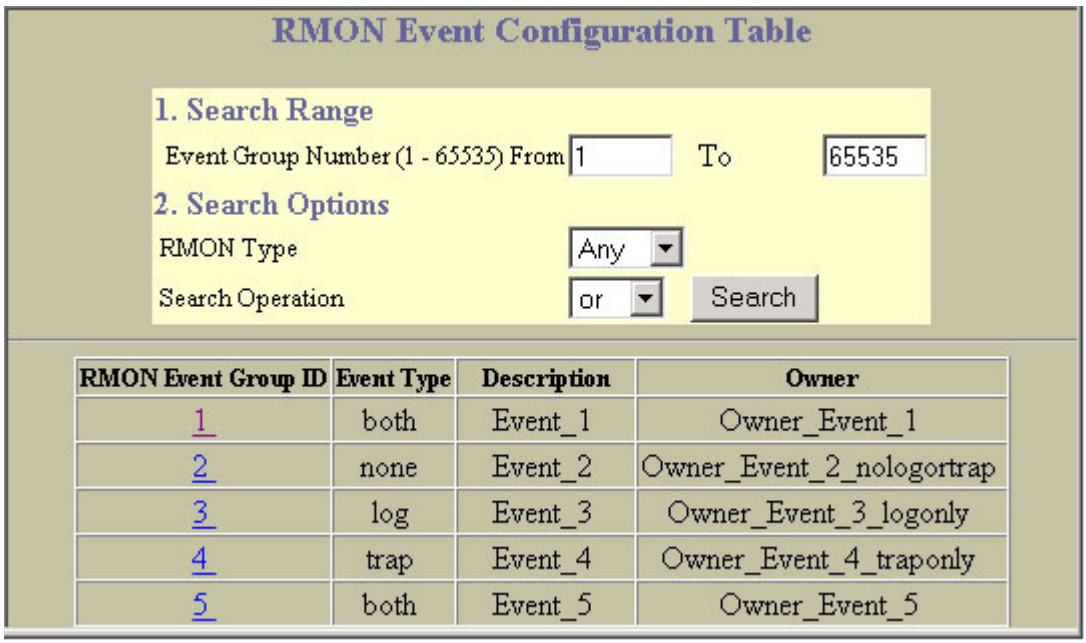
Control	Description
Alarm Group ID	Configures the numeric identifier of the Alarm index.
MIB Object ID	Configures an alarm MIB Object Identifier. The alarm OID can have a maximum of 127 characters.
Rising Limit	Configures the rising threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event is generated.
Falling Limit	Configures the falling threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event is generated.
Rising Event Index	Configures the rising alarm event index that is triggered when a rising threshold is crossed. The range is from 0 to 65535. The default value is 0.
Falling Event Index	Configures the falling alarm event index that is triggered when a falling threshold is crossed. The range is from 0 to 65535. The default value is 0.
Alarm Type	Configures the alarm type as rising, falling, or either (rising or falling).
Sample Type	Configures the method of sampling the selected variable and calculating the value to be compared against the thresholds, as follows: • **abs**: absolute value, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. • **delta**: delta value, the value of the selected variable at the last sample is subtracted from the current value, and the difference compared with the thresholds.
Polling Interval	Configures the time interval over which data is sampled and compared with the rising and falling thresholds. The range is from 1 to 3600 seconds. The default is 1800 seconds.

Table 129 Alarm Group Configuration controls

Control	Description
Owner	Enter a text string that identifies the person or entity that uses this alarm index. The owner can have a maximum of 127 characters.

RMON Event Configuration Table

To display the following form, select **RMON > Event** (click the underlined text, not the folder).



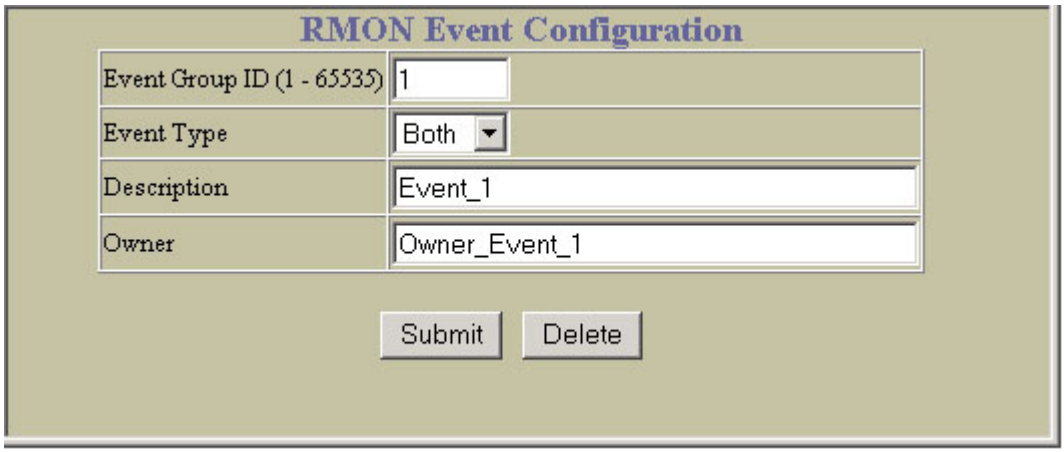
The following table describes the Event Groups Configuration controls:

Table 130 RMON Event Configuration controls

Control	Description
Search Range	To search for a RMON Event Group, enter a range of numbers in the **From** and **To** fields.
Search Options	To focus the search for an Event Group, enter optional search parameters: • RMON Type Fields that have a value of "any" are ignored during the search. Choose a search operation: • **or**: Search for Events specified in the search range that meet any of the criteria entered. • **and**: Search for Events specified in the search range that meet all of the criteria entered. Click **Search** to display Events that fit the range and meet the criteria entered.

RMON Event Configuration

To display the following form, go to the RMON Event Groups Configuration form. Select an Event Group, or open the Event folder and click **Add Event Group.**



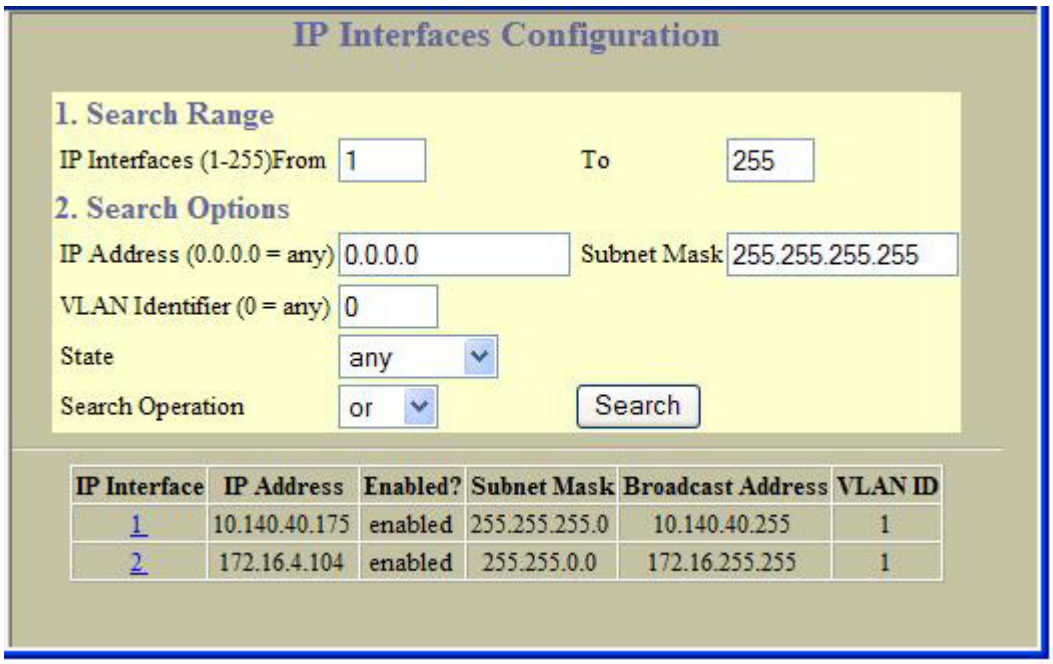
The following table describes the Event Group Configuration controls:

Table 131 Event Group Configuration controls

Control	Description
Event Group ID	Configures the numeric identifier of this Event index.
Event Type	Selects the type of notification provided for this event. For log events, an entry is made in the log table and sent to the configured syslog host. For trap events, an SNMP trap is sent to the management station (`/cfg/snmp/trap`).
Description	Enter a text string to describe the event. The description can have a maximum of 127 characters.
Owner	Enter a text string that identifies the person or entity that uses this Event index. The owner can have a maximum of 127 characters.

IP Interfaces Configuration

To display the following form, select **Layer 3 > IP Interfaces** (click the underlined text, not the folder).



This form summarizes IP Interface parameters.

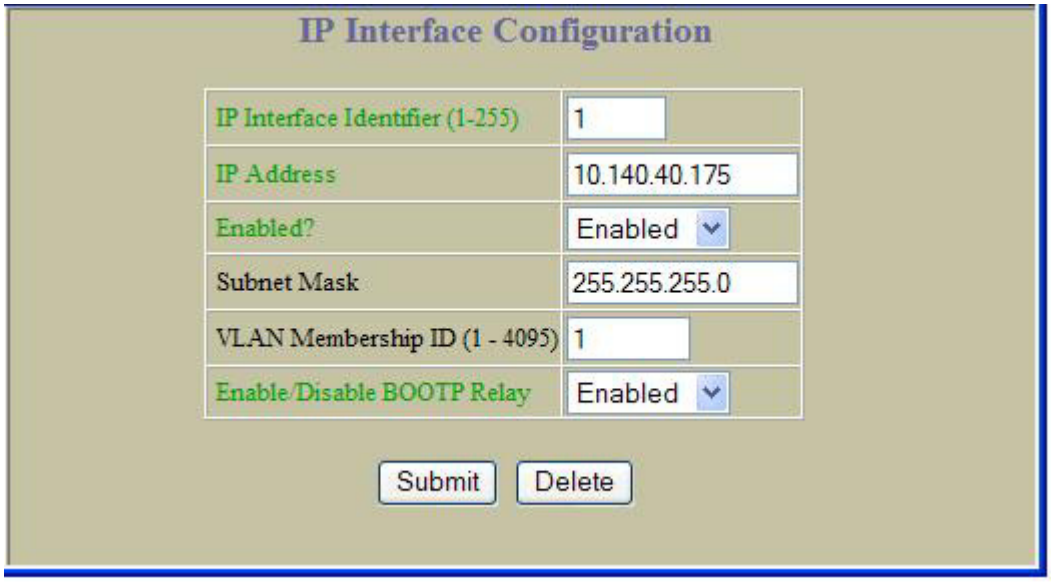
The following table describes IP Interfaces Configuration controls:

Table 132 IP Interfaces Configuration controls

Control	Description
Search Range	To search for an IP Interface, enter a range of IP Interface numbers in the **From** and **To** fields.
Search Options	To focus the search for an IP Interface, enter optional search parameters: • IP Address • Subnet Mask • VLAN ID number • IP Interface State Fields that have a value of "any" are ignored during the search. Choose a search operation: • **or**: Search for IP Interfaces specified in the Search range that meet any of the criteria entered. • **and**: Search for IP Interfaces specified in the Search range that meet all of the criteria entered. Click **Search** to display IP Interfaces that fit the range and meet the criteria entered.

IP Interface Configuration

To display the following form, go to the IP Interfaces Configuration form. Select an IP Interface number, or open the IP Interfaces folder and click **Add IP Interface.**



The GbE2 Interconnect Switch can be configured with up to 255 IP interfaces. Each IP interface represents the GbE2 Interconnect Switch on an IP subnet on your network. The Interface option is disabled by default.

The following table describes the IP Interface Configuration controls:

Table 133 IP Interface Configuration controls

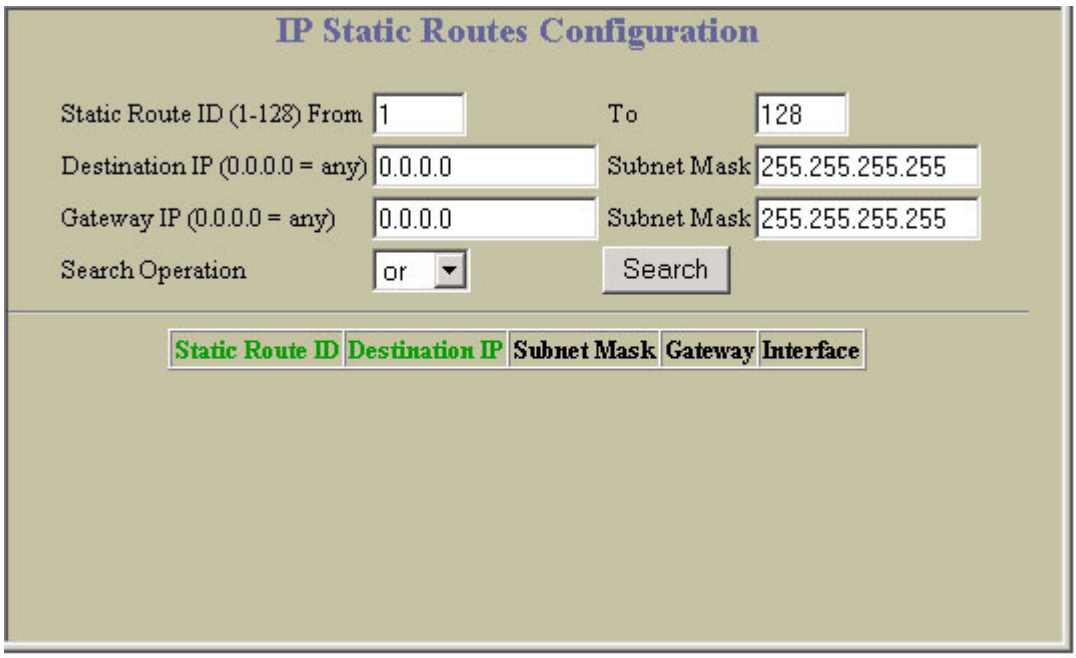
Control	Description
IP Interface Identifier (1-255)	Selects an IP interface to configure.
IP Address	Configures the IP address of the switch interface using dotted decimal notation.
Enabled?	Enables or disables this IP interface.
Subnet Mask	Configures the IP subnet address mask for the interface using dotted decimal notation.
Broadcast Address	Configures the IP broadcast address for the interface using dotted decimal notation.
VLAN Membership ID (1-4095)	Configures the VLAN number for this interface. Each interface can belong to one VLAN, although any VLAN can have multiple IP interfaces in it.

Table 133 IP Interface Configuration controls

Control	Description
Enable/Disable BOOTP Relay	Enables or disables the BOOTP relay on this interface. BOOTP Relay is enabled by default.

IP Static Routes Configuration

To display the following form, select **Layer 3 > Network Routes** (click the underlined text, not the folder).



This form summarizes static route parameters.

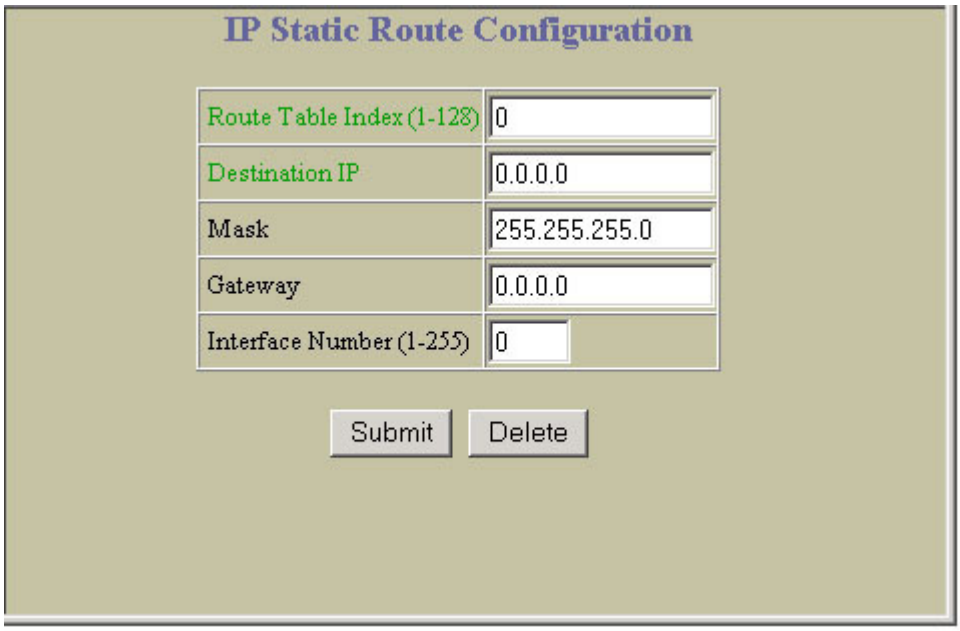
The following table describes IP Static Routes Configuration controls:

Table 134 IP Static Routes Configuration controls

Control	Description
Search Operation	To focus the search for an IP static route, enter search parameters: • Static Route ID • Destination IP address and subnet mask • Gateway IP address and subnet mask Fields that have a value of "any" are ignored during the search. Choose a search operation: • **or**: Search for IP static routes specified in the Search range that meet any of the criteria entered. • **and**: Search for IP static routes specified in the Search range that meet all of the criteria entered. Click **Search** to display IP static routes that fit the range and meet the criteria entered.

IP Static Route Configuration

To display the following form, go to the IP Static Routes Configuration form. Select a static route ID number, or open the Network Routes folder and click **Add Network Route**.



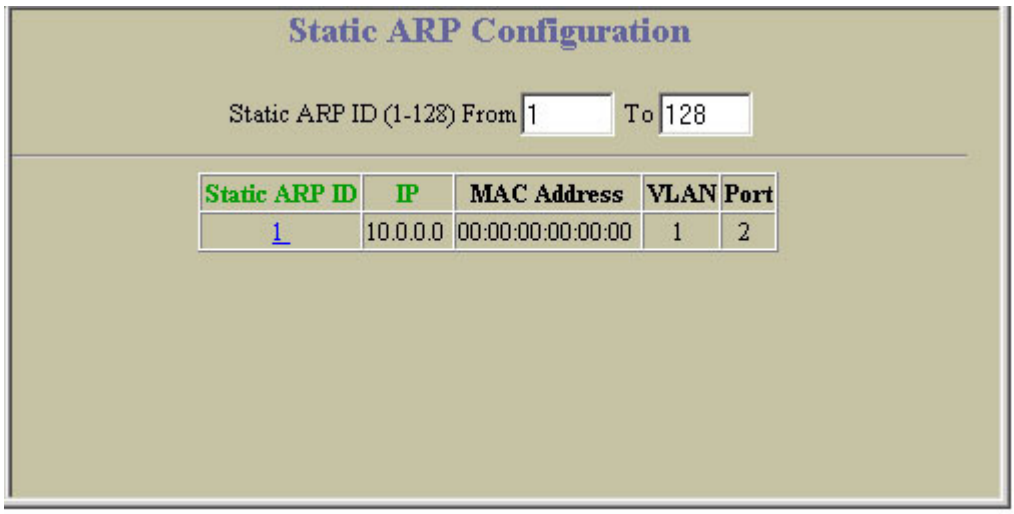
The following table describes the IP Static Route Configuration controls:

Table 135 IP Static Route Configuration controls

Control	Description
Route Table Index (1-128)	Sets the numeric identifier for this index.
Destination IP	Enter the destination IP address for this route.
Mask	Enter the subnet mask for this route.
Gateway	Enter the IP address of the gateway associated with this route.
Interface Number (1-255)	Assigns an interface number to this route.

Static ARP Configuration

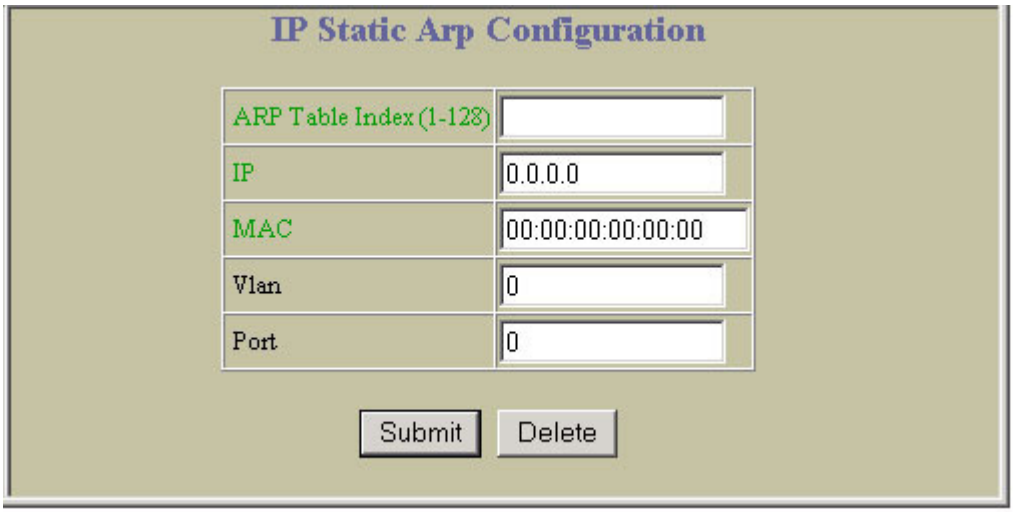
To display the following form, select **Layer 3 > ARP** (click the underlined text, not the folder).



This form summarizes the current static ARP entries. Select a static ARP ID number to display the IP Static ARP Configuration form.

IP Static ARP Configuration

To display the following form, go to the Static ARP Configuration form. Select a static ARP ID number, or open the ARP folder and click **Add Static ARP**.



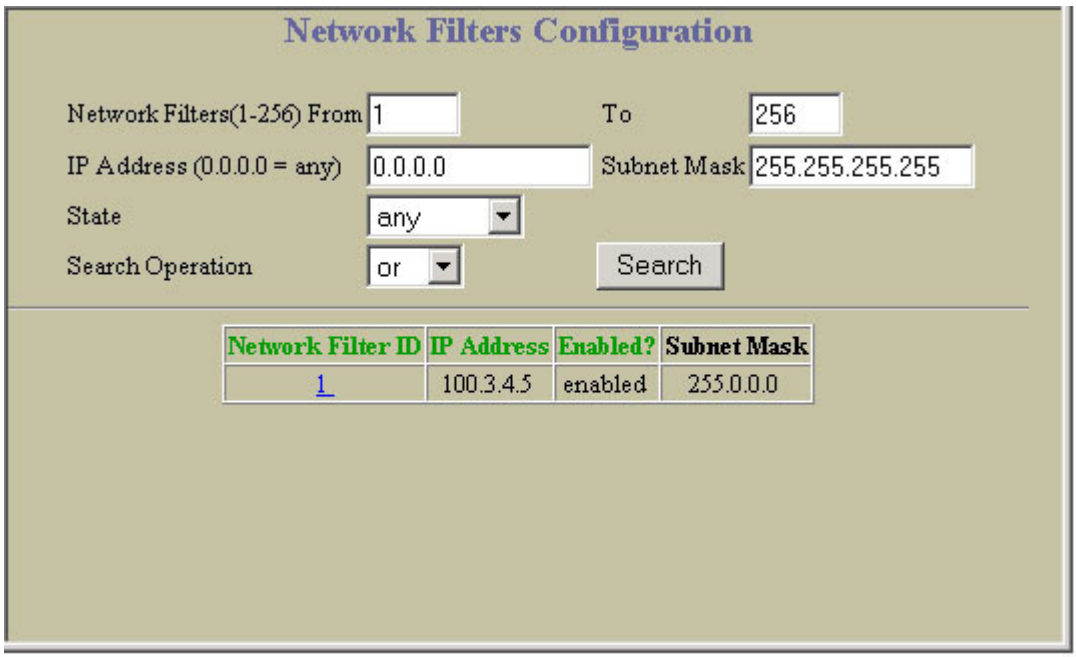
The following table describes ARP Configuration controls:

Table 136 IP Static ARP Configuration controls

Control	Description
ARP Table Index (1-128)	Configures the table index number for the static ARP entry.
IP	Configures the IP address of the host.
MAC	Configures the MAC address of the host.
VLAN	Configures the VLAN ID for the host.
Port	Configures the port to which the host connects.

Network Filters Configuration

To display the following form, select **Layer 3 > Network Filters** (click the underlined text, not the folder).



This form summarizes network filter parameters.

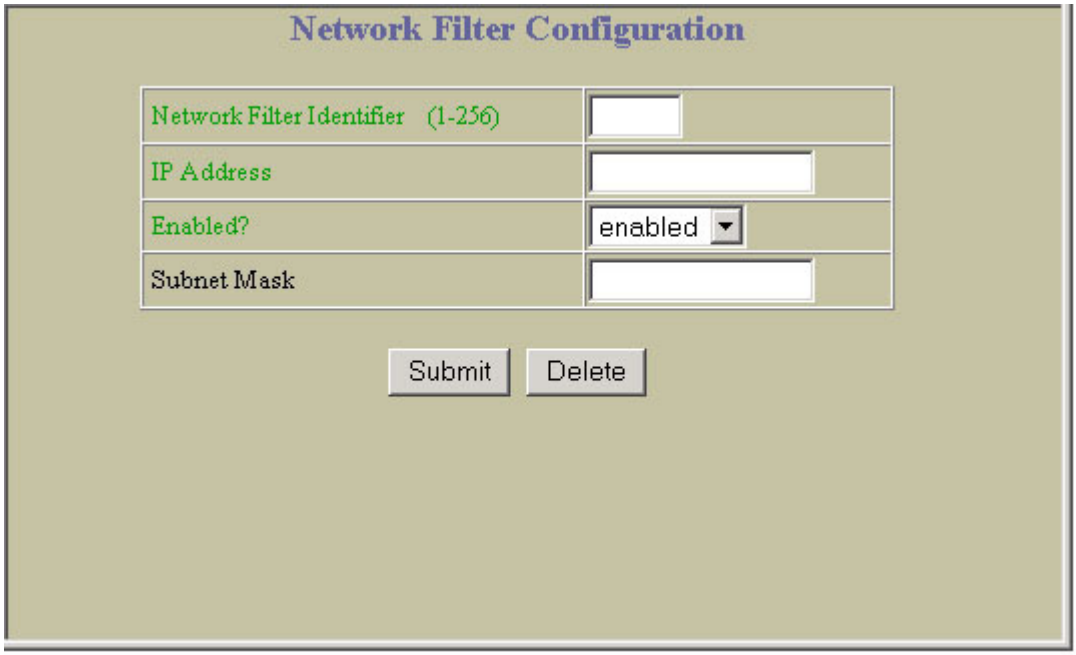
The following table describes Network Filters Configuration controls:

Table 137 Network Filters Configuration controls

Control	Description
Search Operation	To focus the search for a network filter, enter optional search parameters: • Network Filter ID • IP address and subnet mask • State Fields that have a value of "any" are ignored during the search. Choose a search operation: • **or**: Search for network filters specified in the Search range that meet any of the criteria entered. • **and**: Search for network filters specified in the Search range that meet all of the criteria entered. Click **Search** to display network filters that fit the range and meet the criteria entered.

Network Filter Configuration

To display the following form, go to the Network Filters Configuration form. Select a network filter ID number, or open the Network Filters folder and click **Add Network Filter**.



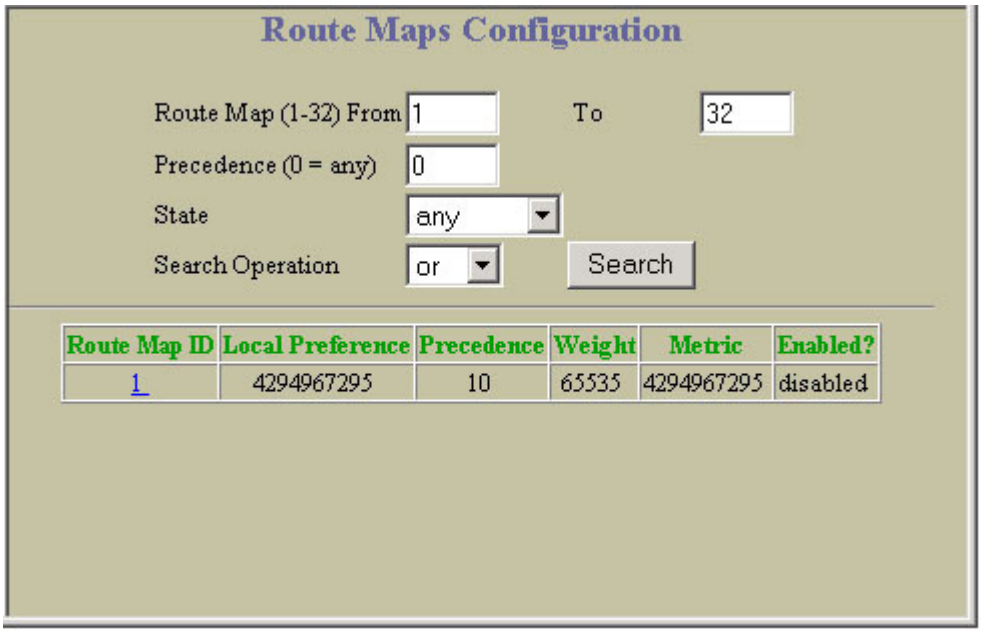
The following table describes the Network Filter Configuration controls:

Table 138 Network Filter Configuration controls

Control	Description
Network Filter Identifier (1-256)	Sets the numeric identifier for this network filter.
IP Address	Sets the starting IP address for this filter. The default address is 0.0.0.0
Enabled?	Enables or disables the Network Filter configuration.
Subnet Mask	Sets the IP subnet mask that is used to define the range of IP addresses that will be accepted by the peer when the filter is enabled. The default value is 0.0.0.0

Route Maps Configuration

To display the following form, select **Layer 3 > Route Maps** (click the underlined text, not the folder).



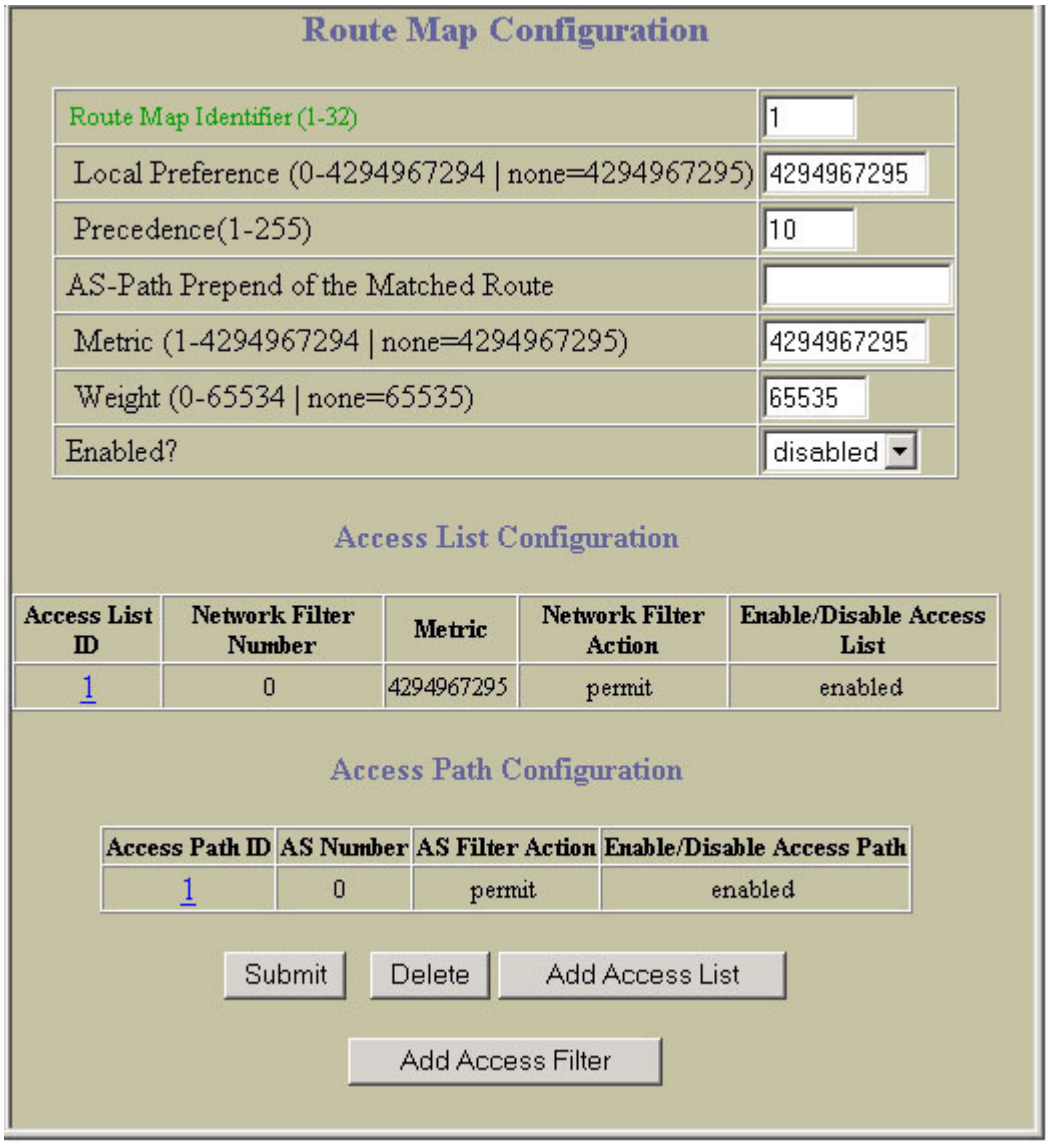
The following table describes Route Maps Configuration controls:

Table 139 Route Maps Configuration controls

Control	Description
Search Operation	To focus the search for a route map, enter optional search parameters: • Route Map ID • Precedence • State Fields that have a value of "any" are ignored during the search. Choose a search operation: • **or**: Search for route maps specified in the Search range that meet any of the criteria entered. • **and**: Search for route maps specified in the Search range that meet all of the criteria entered. Click **Search** to display route maps that fit the range and meet the criteria entered.

Route Map Configuration

To display the following form, go to the Route Maps Configuration form. Select a route map ID number, or open the Route Maps folder and click **Add Route Map**.



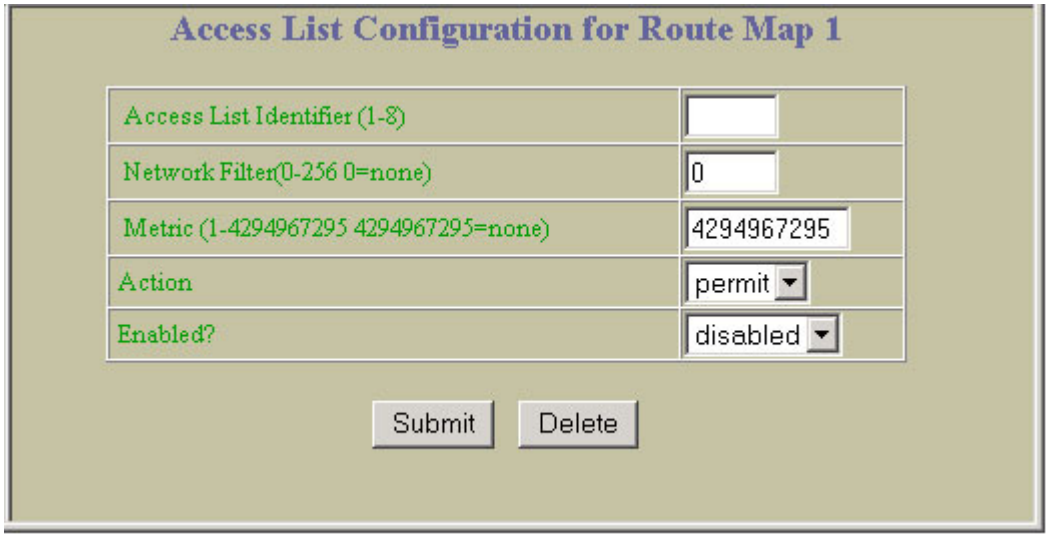
The following table describes the Route Map Configuration controls:

Table 140 Route Map Configuration controls

Control	Description
Route Map Identifier (1-32)	Assigns a numeric identifier to the route map.
Local Preference (1-4294967294 | none=4294967295)	Sets the local preference of the matched route, which affects both inbound and outbound directions. The path with the higher preference is preferred.
Precedence (1-255)	Sets the precedence of the route map. The smaller the value, the higher the precedence. Default value is 10.
AS-Path Prepend of the Matched Route	Sets the AS path preference of the matched route. One to three path preferences can be configured.
Metric (1-4294967294 | none=4294967295)	Sets the metric of the matched route.
Weight (0-65534 | none=65535)	Sets the weight of the route map.
Enabled?	Enables or disables the route map.

Route Map Access List Configuration

To display the following form, go to the Route Map Configuration form. Click **Add Access List.**



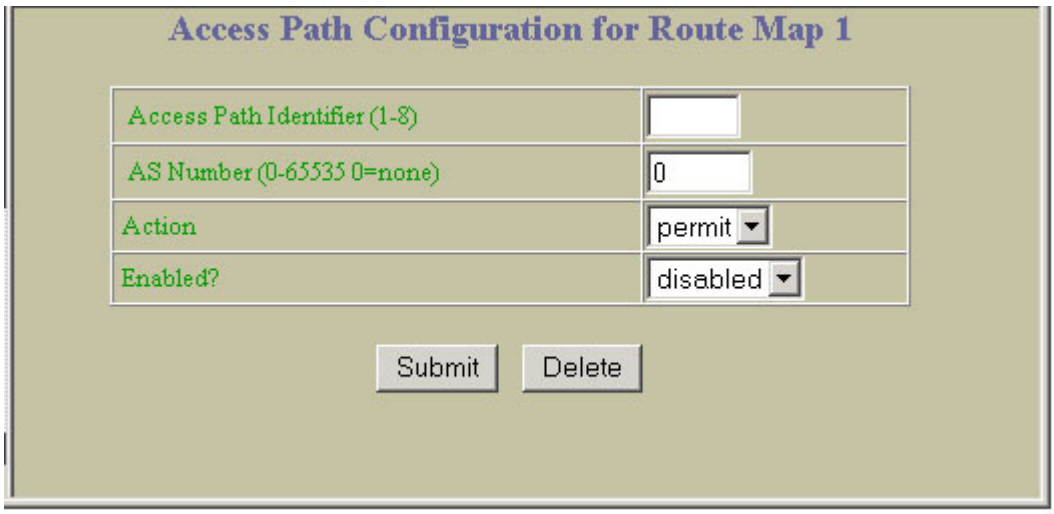
The following table describes the Access List Configuration controls:

Table 141 Access List Configuration controls

Control	Description
Access List Identifier (1-8)	Assigns the access list number.
Network Filter (0-256, 0=none)	Sets the network filter number associated with the access list.
Metric (1-4294967295, 4294967295=none)	Sets the metric value in the AS-External (ASE) LSA.
Action	Permits or denies action for the access list.
Enabled?	Enables or disables the access list.

Route Map Access Path Configuration

To display the following form, go to the Route Map Configuration form. Click **Add Access Filter.**



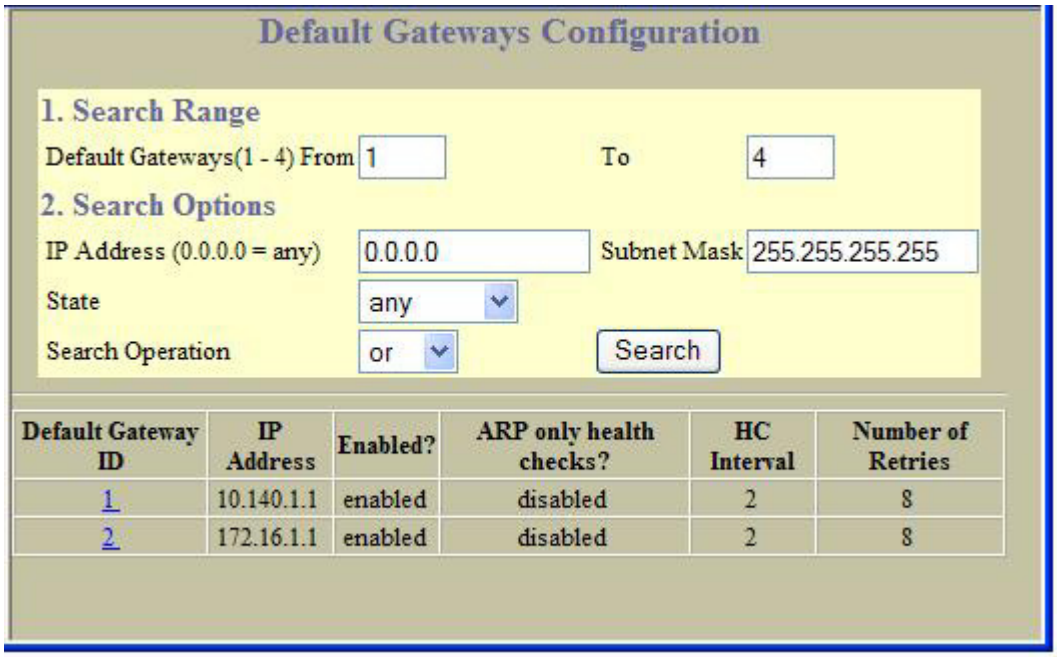
The following table describes the Access Path Configuration controls:

Table 142 Access Path Configuration controls

Control	Description
Access Path Identifier (1-8)	Assigns the access path number.
AS number (0-65535, 0=none)	Sets the Autonomous System filter's path number.
Action	Permits or denies Autonomous System filter action.
Enabled?	Enables or disables the Autonomous System filter.

Default Gateways Configuration

To display the following form, select **IP Menu > Default Gateways** (click the underlined text, not the folder).



This form summarizes default gateway parameters.

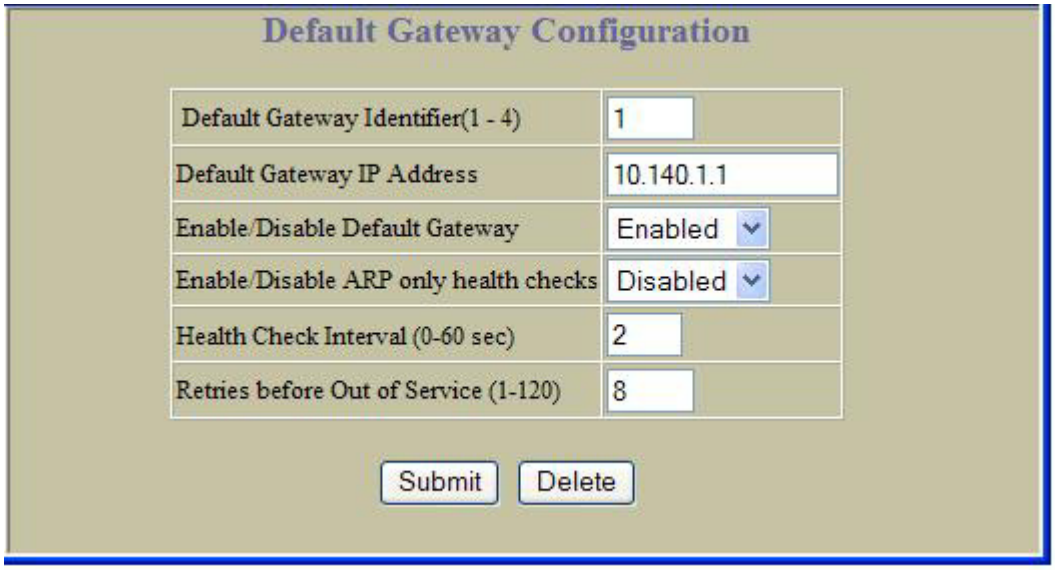
The following table describes the Default Gateways Configuration controls:

Table 143 Default Gateways Configuration controls

Control	Description
Search Range	To search for a Default Gateway, enter a range of Gateway numbers in the **From** and **To** fields.
Search Options	To focus the search for a Default Gateway, enter optional search parameters: • IP Address • Subnet Mask • Default Gateway State Fields that have a value of "any" are ignored during the search. Choose a search operation: • **or**: Search for Default Getaways specified in the search range that meet any of the criteria entered. • **and**: Search for Default Getaways specified in the search range that meet all of the criteria entered. Click **Search** to display Default Getaways that fit the range and meet the criteria entered.

Default Gateway Configuration

To display the following form, go to the Default Gateways Configuration form. Select a Default Gateway ID, or open the Default Gateways folder and click **Add Default Gateway**.



Default Gateways are disabled by default.

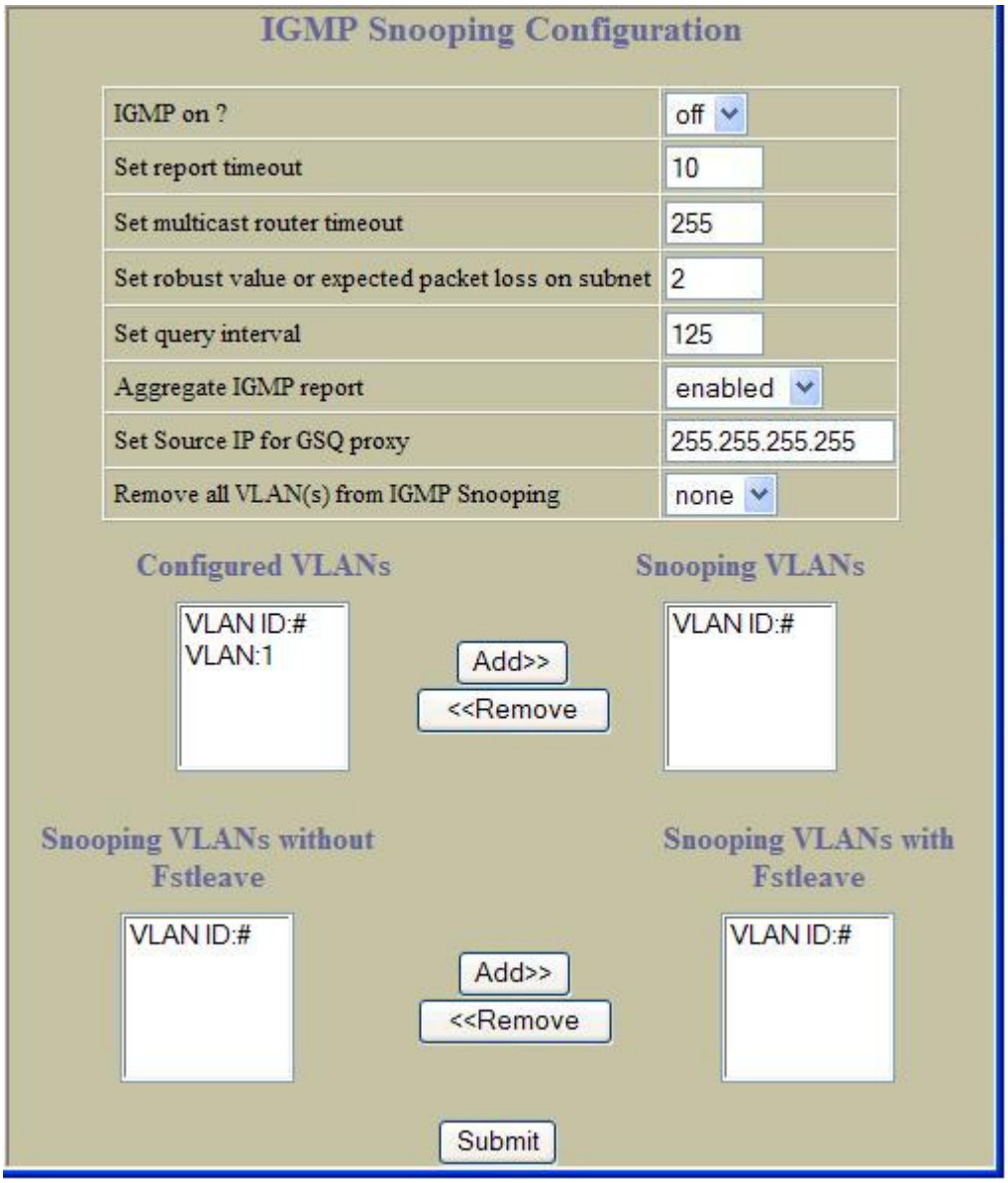
The following table describes the Default Gateway Configuration controls:

Table 144 Default Gateway Configuration controls

Control	Description
Default Gateway Identifier (1-2)	Selects a default Gateway to configure.
Default Gateway IP Address	Configures the IP address of the default IP gateway using dotted decimal notation.
Enable/Disable Default Gateway	Enables or disables the gateway for use.
Enable/Disable ARP only health checks	Enables or disables Address Resolution Protocol (ARP) health checks. This command is disabled by default.
Health Check Interval (0-60 sec)	The switch pings the default gateway to verify that it's up. The **interval** option sets the time between health checks. The range is from 0 to 60 seconds. The default is 2 seconds.
Retries before Out of Service (1-120)	Sets the number of failed health check attempts required before declaring this default gateway inoperative. The range is from 1 to 120 attempts. The default is 8 attempts.

IGMP Snooping Configuration

To display the following form, select **Layer 3 > IGMP > IGMP Snooping** (click the underlined text, not the folder).



Internet Group Management Protocol (IGMP) is used by IP Multicast routers to learn about the existence of host group members on their directly attached subnet (see RFC 2236).

IGMP Snooping allows the switch to forward multicast traffic only to those ports that request it. IGMP Snooping prevents multicast traffic from being flooded to all ports. The switch learns which server hosts are interested in receiving multicast traffic, and forwards it only to ports connected to those servers.

The following table describes the IGMP Snooping Configuration controls:

Table 145 IGMP Snooping Configuration controls

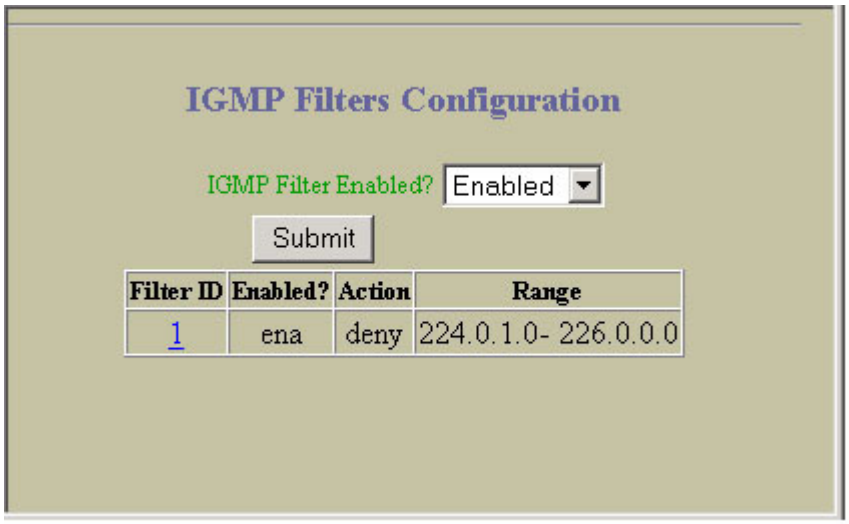
Control	Descriptions
IGMP on?	Enables or disables IGMP Snooping.
Set report timeout	Configures the timeout value for IGMP Membership Reports (host). Once the timeout value is reached, the switch removes the host from its IGMP table, if the conditions are met. The range is from 1 to 255 seconds. The default is 10 seconds.
Set multicast router timeout	Configures the timeout value for IGMP Membership Queries (Mrouter). Once the timeout value is reached, the switch removes the multicast router from its IGMP table, if the proper conditions are met. The range is from 1 to 255 seconds. The default is 255 seconds.

Table 145 IGMP Snooping Configuration controls

Control	Descriptions
Set robust value or expected packet loss on subnet	Configures the IGMP Robustness variable, which allows you to tune the switch for expected packet loss on the subnet. If the subnet is expected to be lossy (high rate of packet loss), increase the value. The range is from 2 to 10. The default value is 2.
Set query interval	Sets the IGMP router query interval, in seconds. The default value is 125.
Aggregate IGMP report	Enables or disables IGMP Membership Report aggregation.
Set Source IP for GSQ proxy	Configures the source IP address used as a proxy for IGMP Group Specific Queries.
Remove all VLAN(s) from IGMP Snooping	Removes all VLANs from the list of Snooping VLANs.
Configured VLANs	Lists the VLANs that can be assigned for IGMP Snooping.
Snooping VLANs	Enables or disables IGMP Snooping on selected VLANs. **Add**: Adds selected VLANs to the Snooping VLANs list. To add a VLAN, select the VLAN in the Configured VLANs list, and click **Add.** **Remove**: Removes selected VLANs from the Snooping VLANs list.
Snooping VLANs without Fstleave	Lists the Snooping VLANs that can be assigned for Fstleave processing.
Snooping VLANs with Fstleave	Enables or disables Fastleave processing. Fastleave allows the switch to immediately remove a port from the IGMP port list, if the host sends a Leave message, and the proper conditions are met. This command is disabled by default. **Add**: Adds selected VLANs to the Snooping VLANs with Fstleave list. To add a VLAN, select the VLAN in the Snooping VLANs without Fstleave list, and click **Add.** **Remove**: Removes selected VLANs from the Snooping VLANs with Fstleave list.

IGMP Filters Configuration

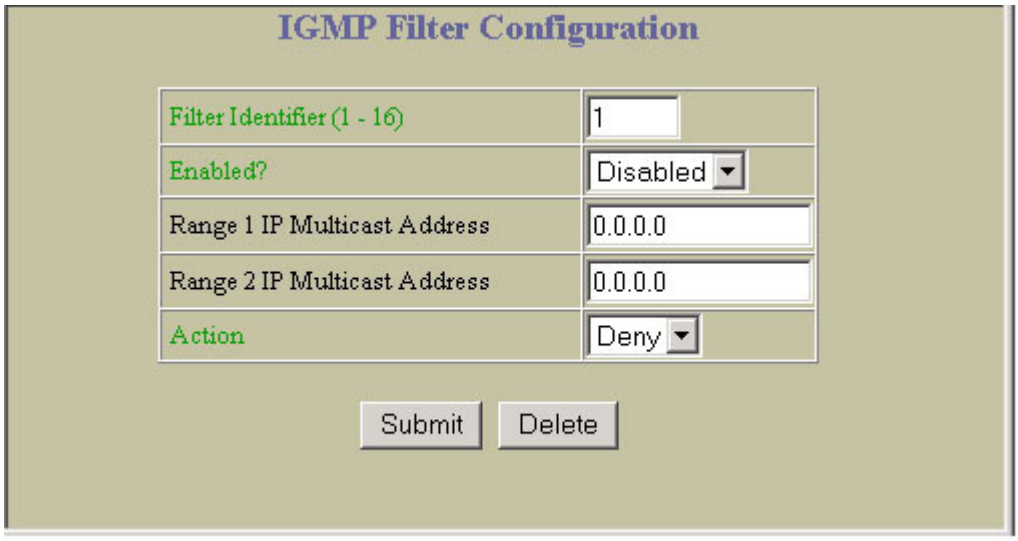
To display the following form, select **Layer 3 > IGMP > IGMP Filters** (click the underlined text, not the folder).



This form summarizes IGMP filter parameters. Use IGMP filters to allow or deny a port to send and receive multicast traffic.

IGMP Filter Configuration

To display the following form, go to the IGMP Filters Configuration form. Select a Filter ID, or open the IGMP Filters folder and click **Add Filter**.



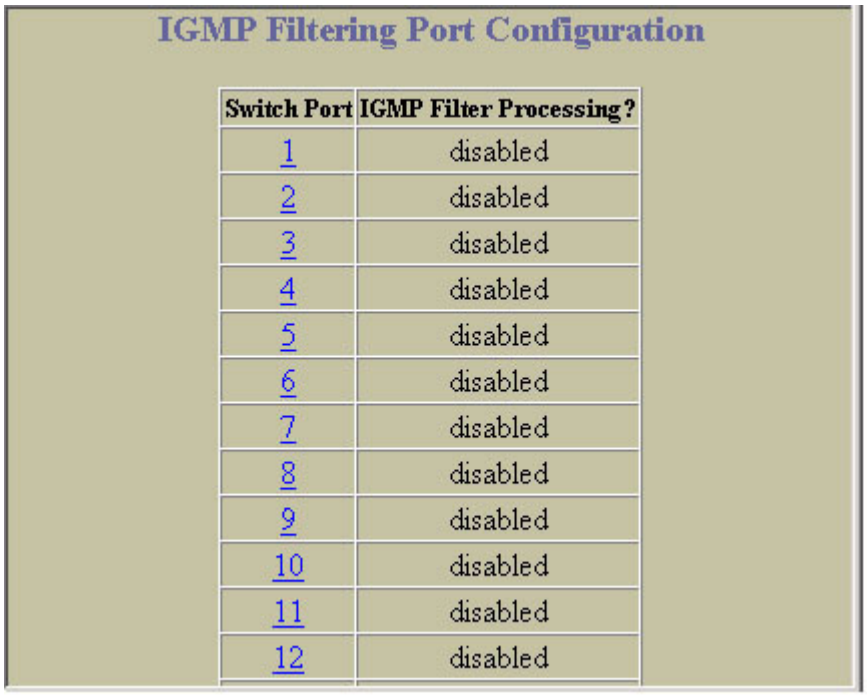
The following table describes the IGMP Filter Configuration controls:

Table 146 IGMP Filter Configuration controls

Control	Description
Filter Identifier (1-16)	Selects an IGMP filter to configure.
Enabled?	Enables or disables this IGMP filter.
Range 1 IP Multicast Address	Configures the start of the range of IP multicast addresses for this filter.
Range 2 IP Multicast Address	Configures the end of the range of IP multicast addresses for this filter.
Action	Allows or denies multicast traffic for the IP multicast address range specified.

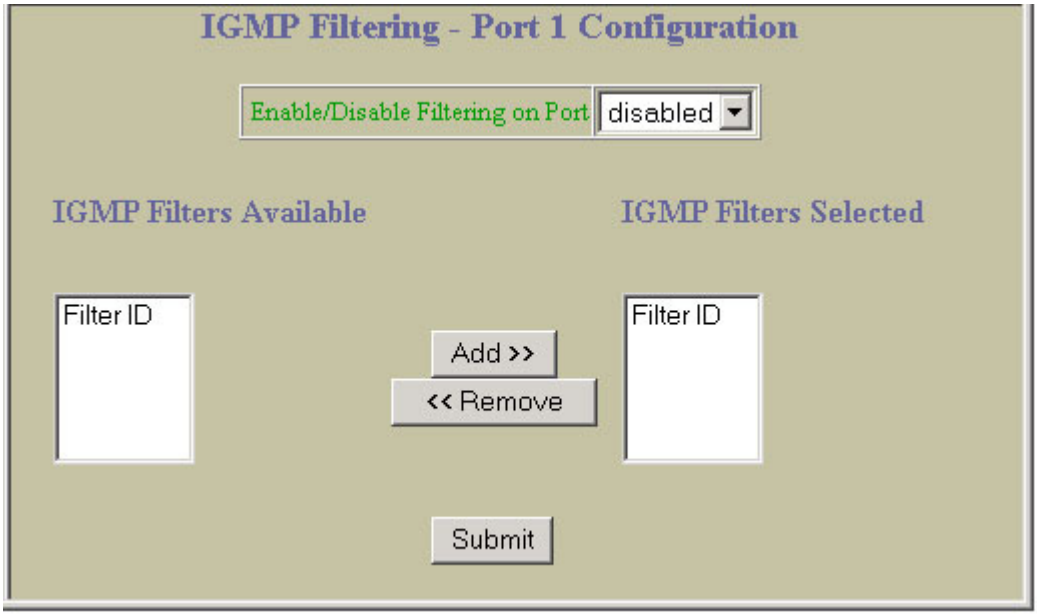
IGMP Filtering Port Configuration

To display the following form, select **Layer 3 > IGMP > Switch Ports**.



IGMP Filtering - Port Configuration

To display the following form, go to the IGMP Filtering Port Configuration form. Select a Switch Port number.



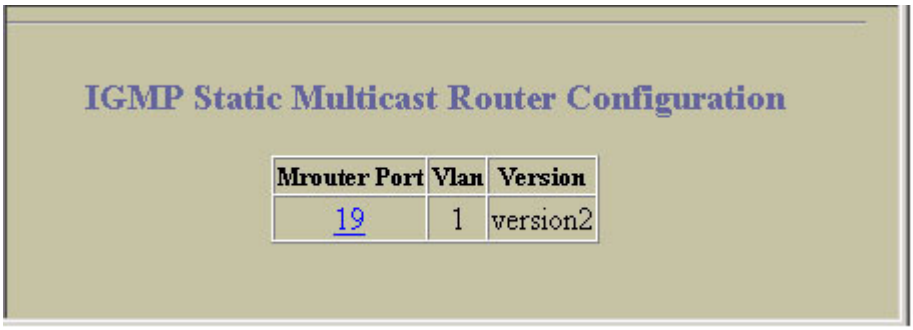
The following table describes IGMP Filtering – Port Configuration controls:

Table 147 IGMP Filtering - Port Configuration controls

Control	Description
Enable/Disable Filtering on Port	Enables or disables IGMP filtering on the port.
IGMP Filters Available	Lists the filters that you can add to the port.
IGMP Filters Selected	Lists the filters that have been added to the port. Select a filter number in the IGMP Filters Available list and click **Add** to add the filter to the port. Select a filter number in the IGMP Filters Selected list and click **Remove** to remove the filter from the port.

IGMP Static Multicast Router Configuration

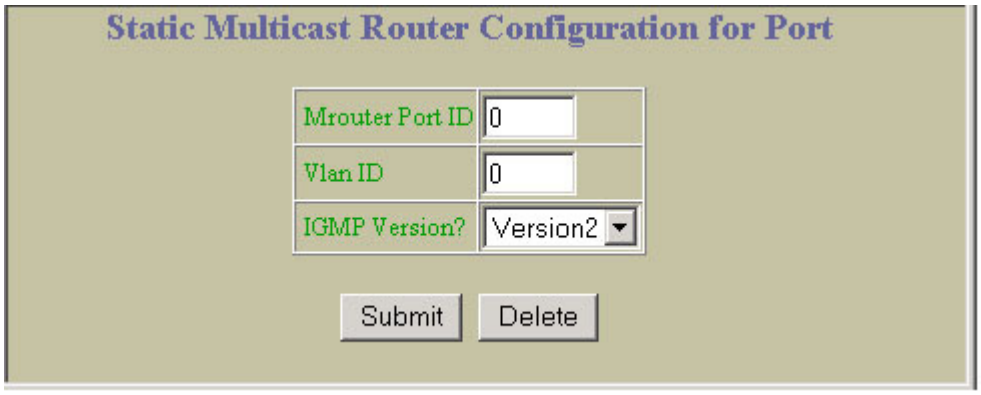
To display the following form, select **Layer 3 > IGMP > IGMP Static MRouter** (click the underlined text, not the folder).



This form provides a summary of configured Static Multicast Routers.

Static Multicast Router Configuration for Port

To display the following form, go to the IGMP Static Multicast Router Configuration form. Select an Mrouter Port number, or open the IGMP Static Mrouter folder and click **Add Mrouter**.



NOTE: When you configure a static multicast router on a VLAN, the process of learning multicast routers is disabled for that VLAN.

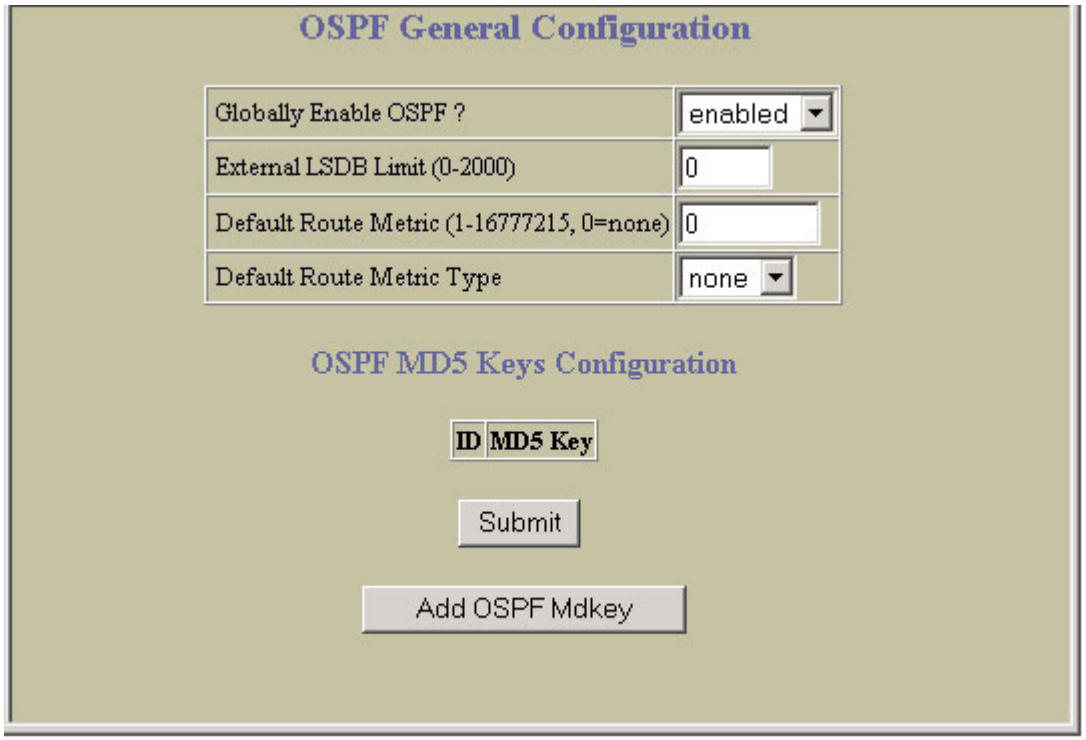
The following table describes the Static Multicast Router Configuration for Port controls:

Table 148 Static Multicast Router Configuration for Port controls

Control	Description
Mrouter Port ID	Selects a port on which the static multicast router is connected.
NOTE: Port number must be an external port (17-24).	
Vlan ID	Selects a VLAN on which the static multicast router is connected.
IGMP Version?	Configures the IGMP version (1 or 2) of the multicast router.

OSPF General Configuration

To display the following form, select **Layer 3 > OSPF Routing Protocol > General**.



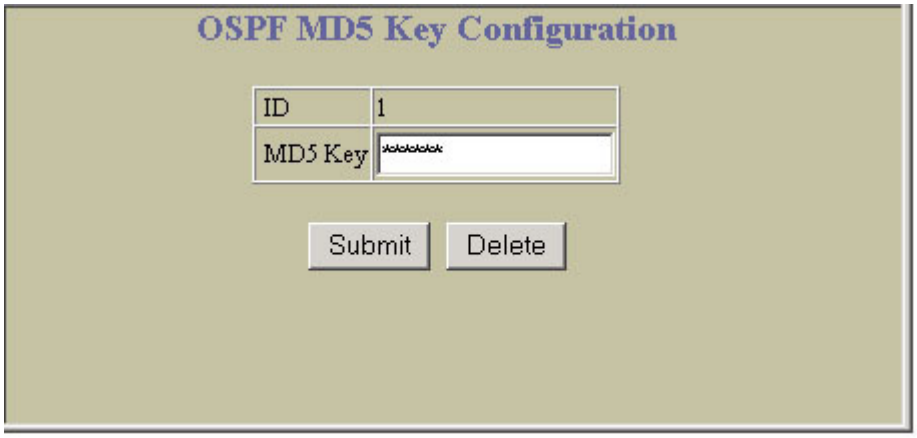
The following table describes the OSPF General Configuration controls:

Table 149 OSPF General Configuration controls

Control	Descriptions
Globally Enable OSPF?	Enables or disables OSPF.
External LSDB Limit (0-2000)	Sets the link state database limit. Enter zero (0) to indicate that there is no limit.
Default Route Metric (1-16777215, 0=none)	Sets one default route among multiple choices in an area.
Default Route Metric Type	Sets the default-route metric type. Enter `none` to indicate that there is no default.

OSPF MD5 Key Configuration

To display the following form, go to the OSPF General Configuration form. Click **Add OSPF Mdkey**.



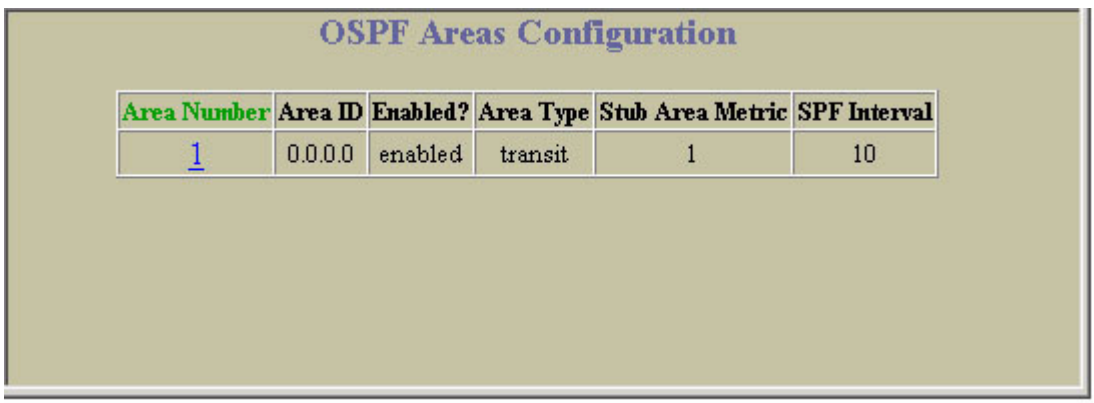
The following table describes the OSPF MD5 Key Configuration controls:

Table 150 OSPF MD5 Key Configuration controls

Control	Descriptions
ID	Displays a numeric identifier for the MD5 authentication key.
MD5 Key	Assigns a string to the MD5 authentication key.

OSPF Areas Configuration

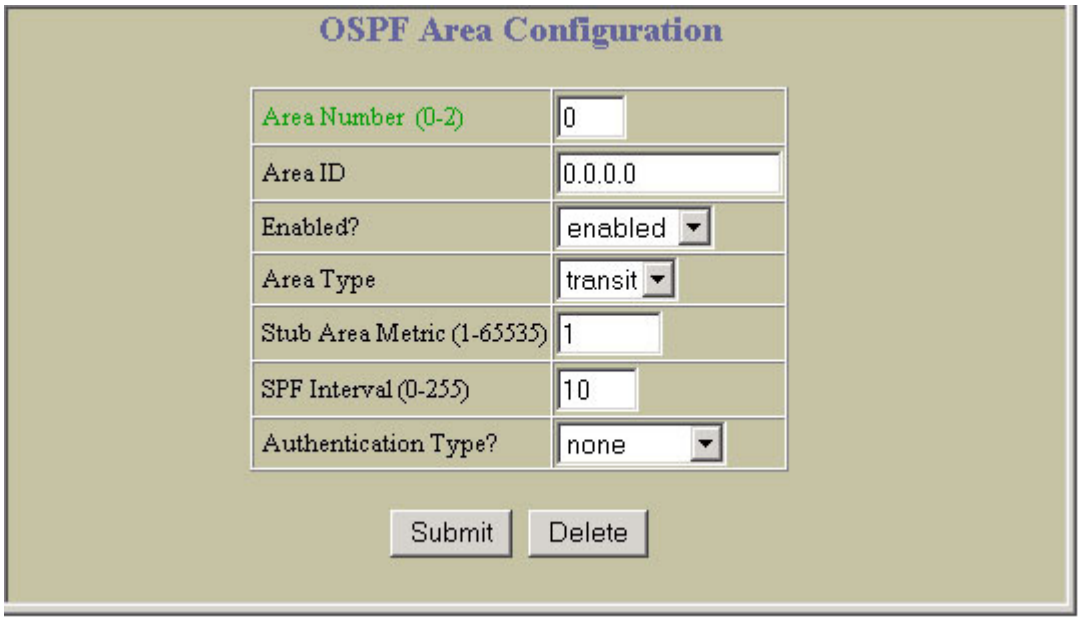
To display the following form, select **Layer 3 > OSPF Routing Protocol > OSPF Areas** (click the underlined text, not the folder).



This form provides a summary of the state of OSPF areas. Select an area number to view the OSPF Area Configuration form.

OSPF Area Configuration

To display the following form, go to the OSPF Areas Configuration form. Select an area number, or open the OSPF Areas folder and click **Add OSPF Area**.



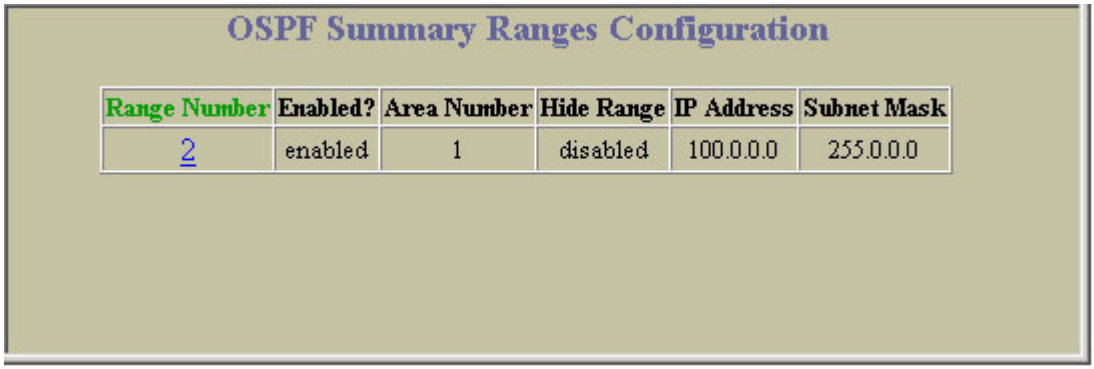
The following table describes the OSPF Area Configuration controls:

Table 151 OSPF Area Configuration controls

Control	Descriptions
Area number (0-2)	Assigns a numeric identifier for the OSPF area.
Area ID	Defines the IP address of the OSPF area number.
Enabled?	Enables or disables the OSPF area.
Area Type	Defines the type of area. For example, when a virtual link has to be established with the backbone, the area type must be defined as transit. • **Transit area:** allows area summary information to be exchanged between routing devices. Any area that is not a stub area or NSSA is considered to be transit area. • **Stub area:** is an area where external routing information is not distributed. Typically, a stub area is connected to only one other area. • **NSSA:** Not-So-Stubby Area (NSSA) is similar to stub area with additional capabilities. For example, routes originating from within the NSSA can be propagated to adjacent transit and backbone areas. External routes from outside the Autonomous System (AS) can be advertised within the NSSA but are not distributed into other areas.
Stub Area Metric (1-65535)	Configures a stub area to send a numeric metric value. All routes received via that stub area carry the configured metric to potentially influencing routing decisions. Metric value assigns the priority for choosing the switch for default route. Metric type determines the method for influencing routing decisions for external routes.
SPF Interval (0-255)	Sets time interval between two successive SPF (shortest path first) calculations of the shortest path tree using the Dijkstra's algorithm.
Authentication Type?	Defines the authentication method, as follows: • **None:** No authentication required. • **Password:** Authenticates simple passwords so that only trusted routing devices can participate. • **MD5:** This parameter is used when MD5 cryptographic authentication is required.

OSPF Summary Ranges Configuration

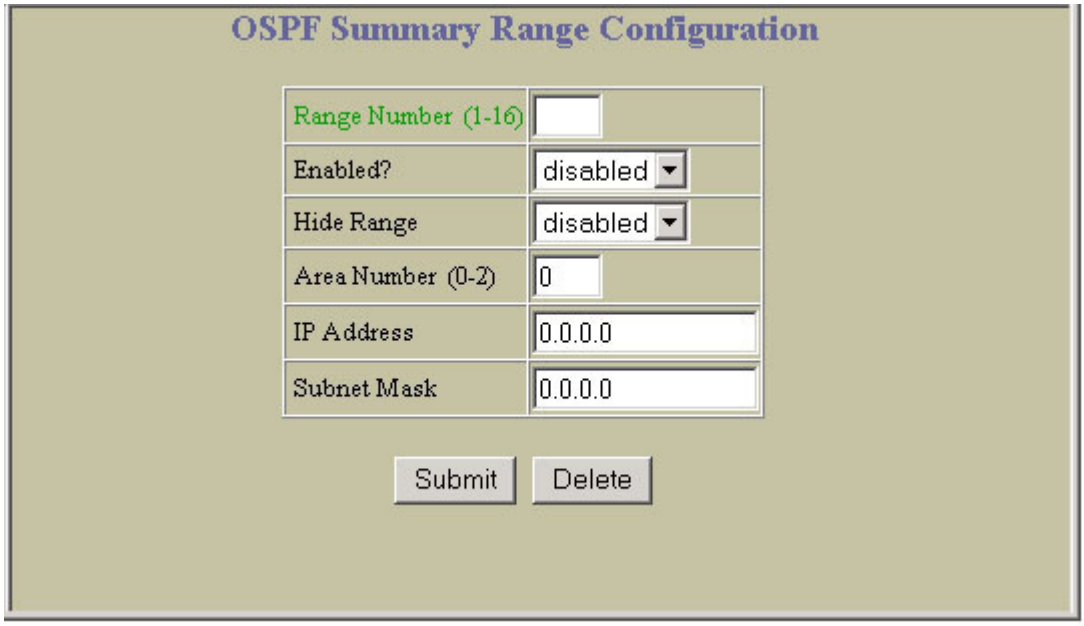
To display the following form, select **Layer 3 > OSPF Routing Protocol > OSPF Summary Ranges** (click the underlined text, not the folder).



This form provides a summary of the state of OSPF summary ranges.

OSPF Summary Range Configuration

To display the following form, go to the OSPF Summary Ranges Configuration form. Select a summary range number, or open the OSPF Summary Ranges folder and click **Add Summary Range**.



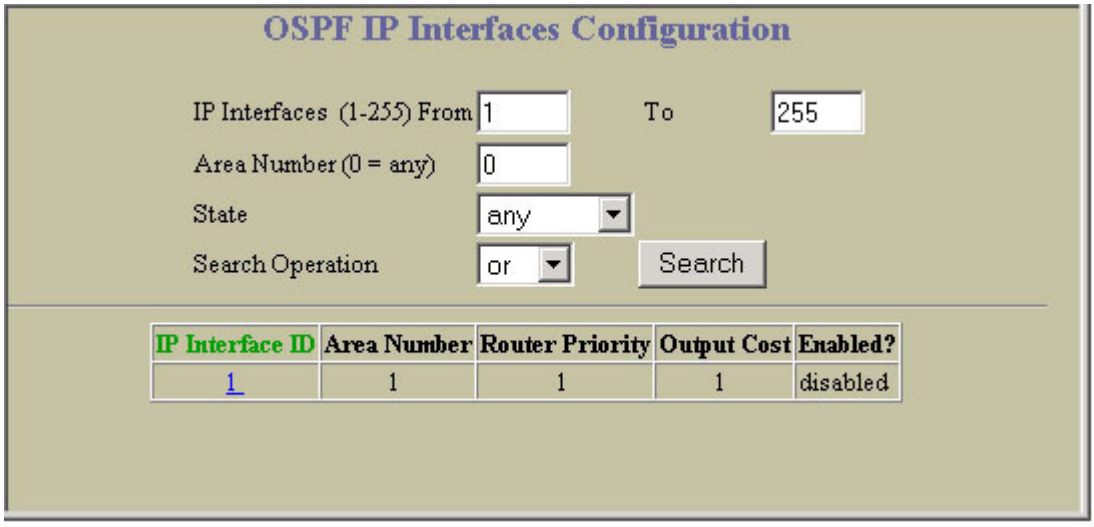
The following table describes the OSPF Summary Range Configuration controls:

Table 152 OSPF Summary Range Configuration controls

Control	Descriptions
Range Number (1-16)	Assigns a numeric identifier to the OSPF summary range.
Enabled?	Enables or disables the OSPF summary range.
Hide Range	Hides or shows the OSPF summary range.
Area number (0-2)	Defines the area index used by the switch.
IP Address	Defines the base IP address for the range.
Subnet Mask	Defines the IP address mask for the range.

OSPF Interfaces Configuration

To display the following form, select **Layer 3 > OSPF Routing Protocol > OSPF Interfaces** (click the underlined text, not the folder).



This form provides a summary of the state of OSPF interfaces.

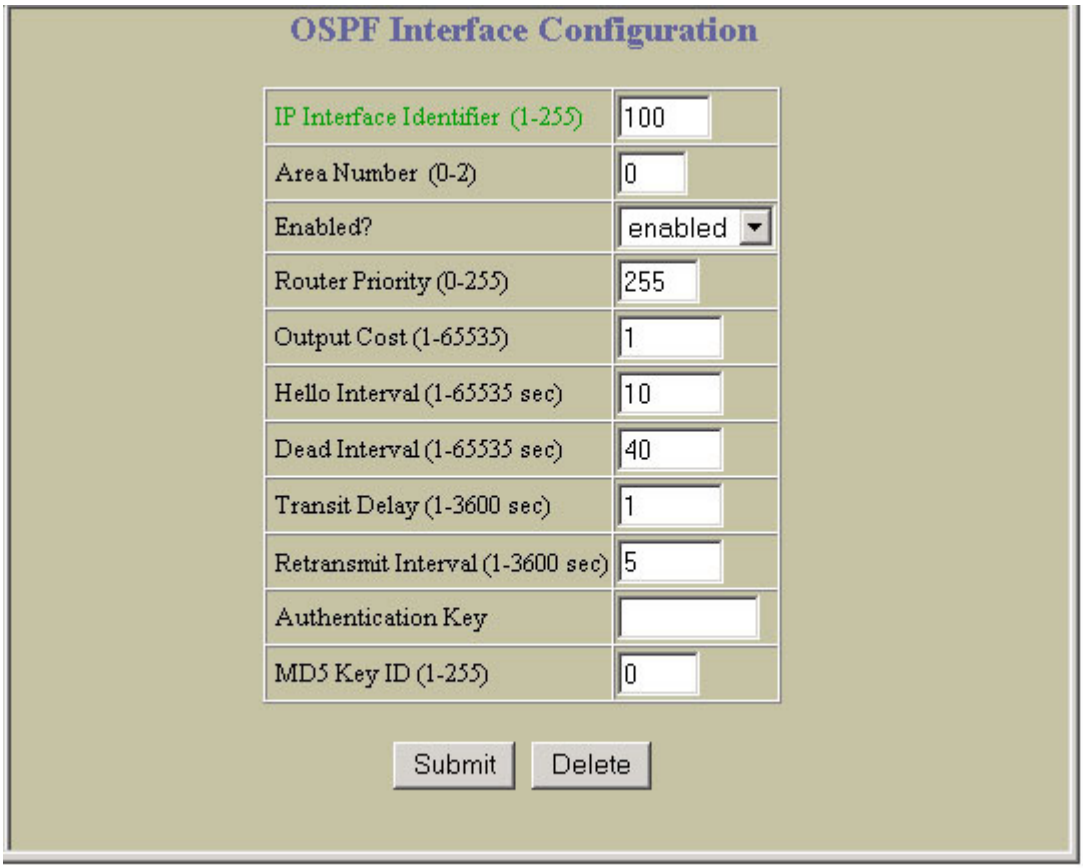
The following table describes OSPF Interfaces Configuration controls:

Table 153 OSPF Interfaces Configuration controls

Control	Description
Search Operation	To focus the search for an OSPF interface, enter search parameters: • IP interfaces • Area Number • State Fields that have a value of "any" are ignored during the search. Choose a search operation: • **or**: Search for OSPF interfaces specified in the Search range that meet any of the criteria entered. • **and**: Search for OSPF interfaces specified in the Search range that meet all of the criteria entered. Click **Search** to display OSPF interfaces that fit the range and meet the criteria entered.

OSPF Interface Configuration

To display the following form, go to the OSPF Interfaces Configuration form. Select an interface number, or open the OSPF Interfaces folder and click **Add OSPF Interface**.



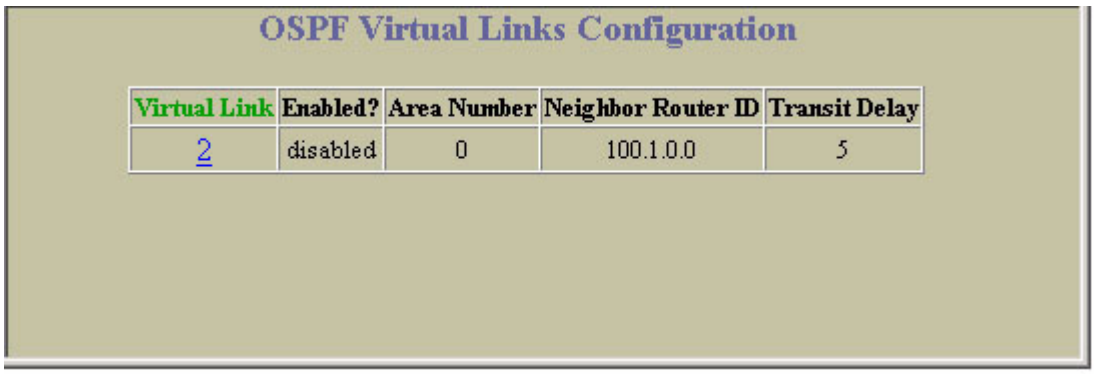
The following table describes the OSPF Interface Configuration controls:

Table 154 OSPF Interface Configuration controls

Control	Descriptions
IP Interface Identifier (1-255)	Assigns a numeric identifier to the OSPF IP interface.
Area Number (0-2)	Defines the area index used by the interface.
Enabled?	Enables or disables the OSPF interface.
Router Priority (0-255)	Displays the assigned priority value to the OSPF interfaces. (A priority value of 127 is the highest and 1 is the lowest. A priority value of 0 specifies that the interface cannot be used as Designated Router (DR) or Backup Designated Router (BDR).)
Output Cost (1-65535)	Displays cost set for the selected path—preferred or backup. Usually the cost is inversely proportional to the bandwidth of the interface. Low cost indicates high bandwidth.
Hello Interval (1-65535 sec)	Displays the interval in seconds between the `hello` packets for the interfaces.
Dead Interval (1-65535 sec)	Displays the health parameters of a `hello` packet, which is set for an interval of seconds before declaring a silent router to be down.
Transit Delay (1-3600 sec)	Displays the transit delay in seconds.
Retransmit Interval (1-3600 sec)	Displays the retransmit interval in seconds.
Authentication Key	Sets the authentication key to clear the password.
MD5 Key ID (1-255)	Assigns an MD5 key to the interface.

OSPF Virtual Links Configuration

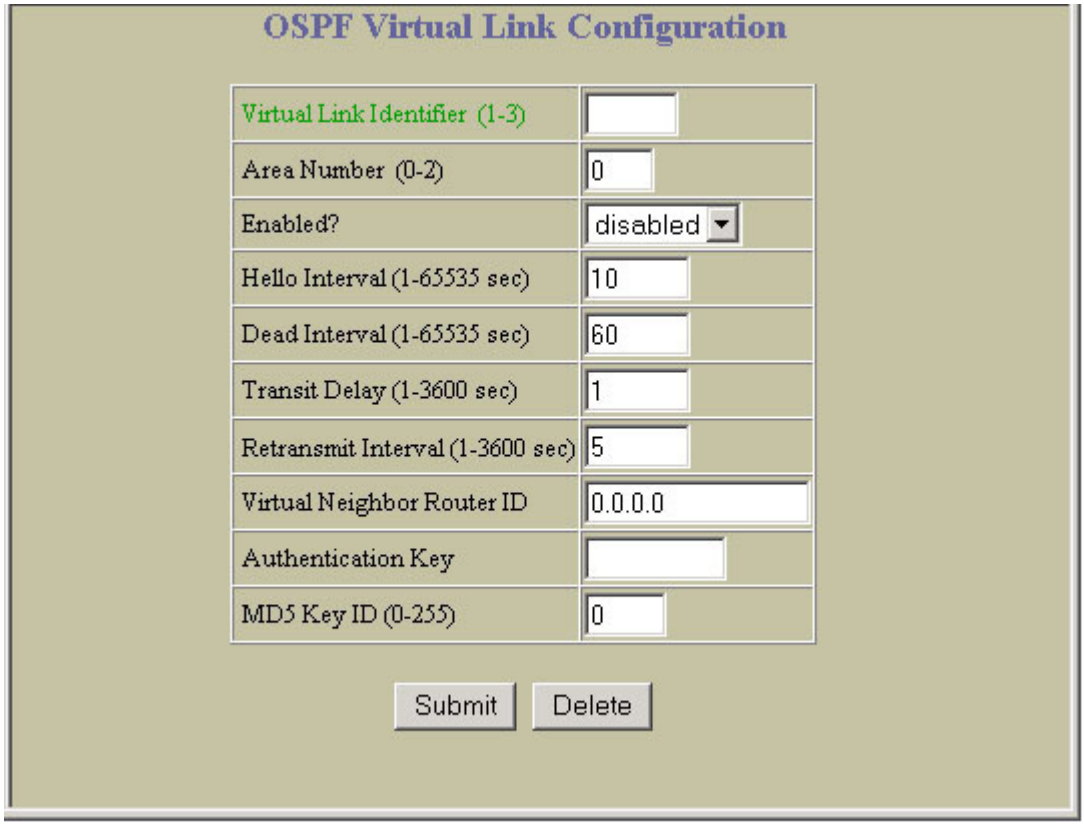
To display the following form, select **Layer 3 > OSPF Routing Protocol > OSPF Virtual Links** (click the underlined text, not the folder).



This form provides a summary of the state of OSPF virtual links.

OSPF Virtual Link Configuration

To display the following form, go to the OSPF Virtual Links Configuration form. Select a virtual link number, or open the OSPF Virtual Links folder and click **Add OSPF Virtual Link**.



The following table describes the OSPF Virtual Link Configuration controls:

Table 155 OSPF Virtual Link Configuration controls

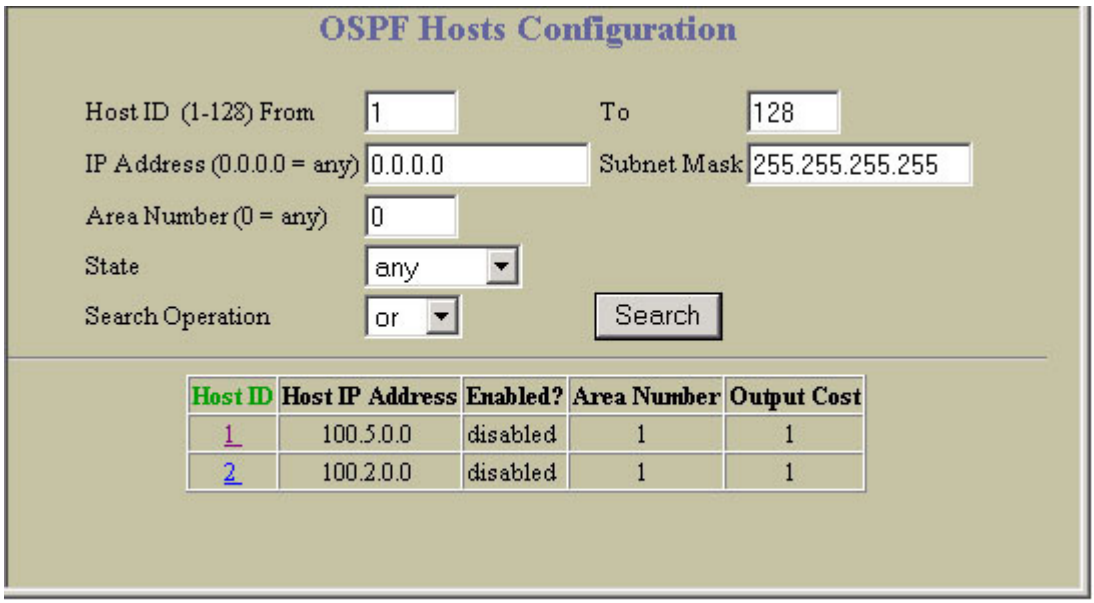
Control	Descriptions
Virtual Link Identifier (1-3)	Assigns a numeric identifier to the virtual link.
Area Number (0-2)	Defines the area index used by the virtual link.
Enabled?	Enables or disables the OSPF virtual link.
Hello Interval (1-65535 sec)	Displays the authentication parameters of a hello packet, which is set to be in an interval of seconds.

Table 155 OSPF Virtual Link Configuration controls

Control	Descriptions
Dead Interval (1-65535 sec)	Displays the health parameters of a hello packet, which is set to be in an interval of seconds. Default is 40 seconds.
Transmit Delay (1-3600 sec)	Displays the delay in transit in seconds. Default is one second.
Retransmit Interval (1-3600 sec)	Displays the retransmit interval in seconds. Default is five seconds.
Virtual Neighbor Router ID	Displays the router ID of the virtual neighbor. Default is 0.0.0.0
Authentication Key	Displays the password (up to eight characters) for each virtual link. Default is none.
MD5 Key ID (0-255)	Sets MD5 key ID for each virtual link. Default is 0 (none).

OSPF Hosts Configuration

To display the following form, select **Layer 3 > OSPF Routing Protocol > OSPF Hosts** (click the underlined text, not the folder).



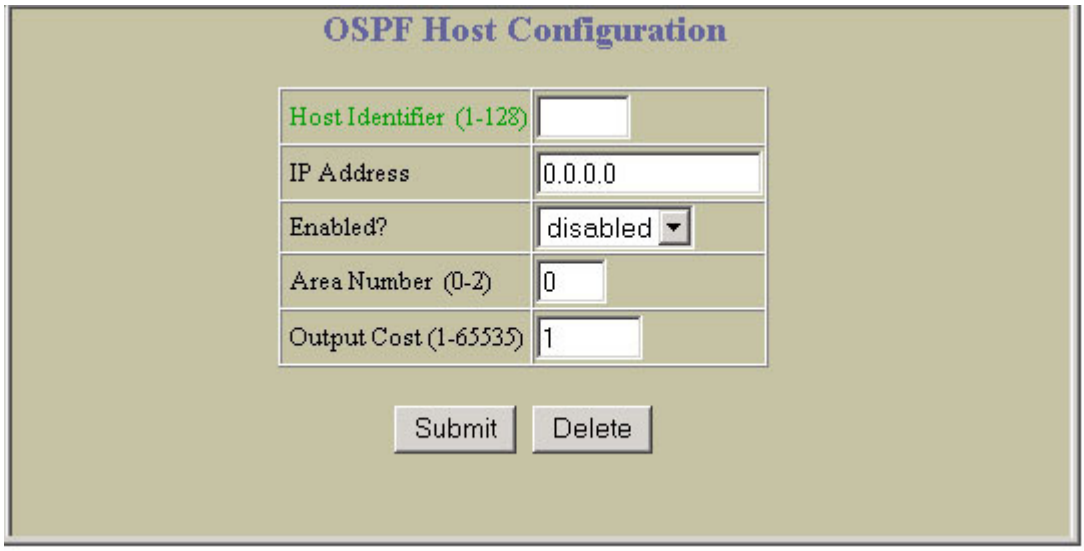
The following table describes OSPF Hosts Configuration controls:

Table 156 OSPF Hosts Configuration controls

Control	Description
Search Operation	To focus the search for an OSPF host, enter search parameters: • Host ID • IP address and subnet mask • Area number • State Fields that have a value of "any" are ignored during the search. Choose a search operation: • **or**: Search for OSPF hosts specified in the Search range that meet any of the criteria entered. • **and**: Search for OSPF hosts specified in the Search range that meet all of the criteria entered. Click **Search** to display OSPF hosts that fit the range and meet the criteria entered.

OSPF Host Configuration

To display the following form, go to the OSPF Hosts Configuration form. Select a host number, or open the OSPF Hosts folder and click **Add OSPF Host**.



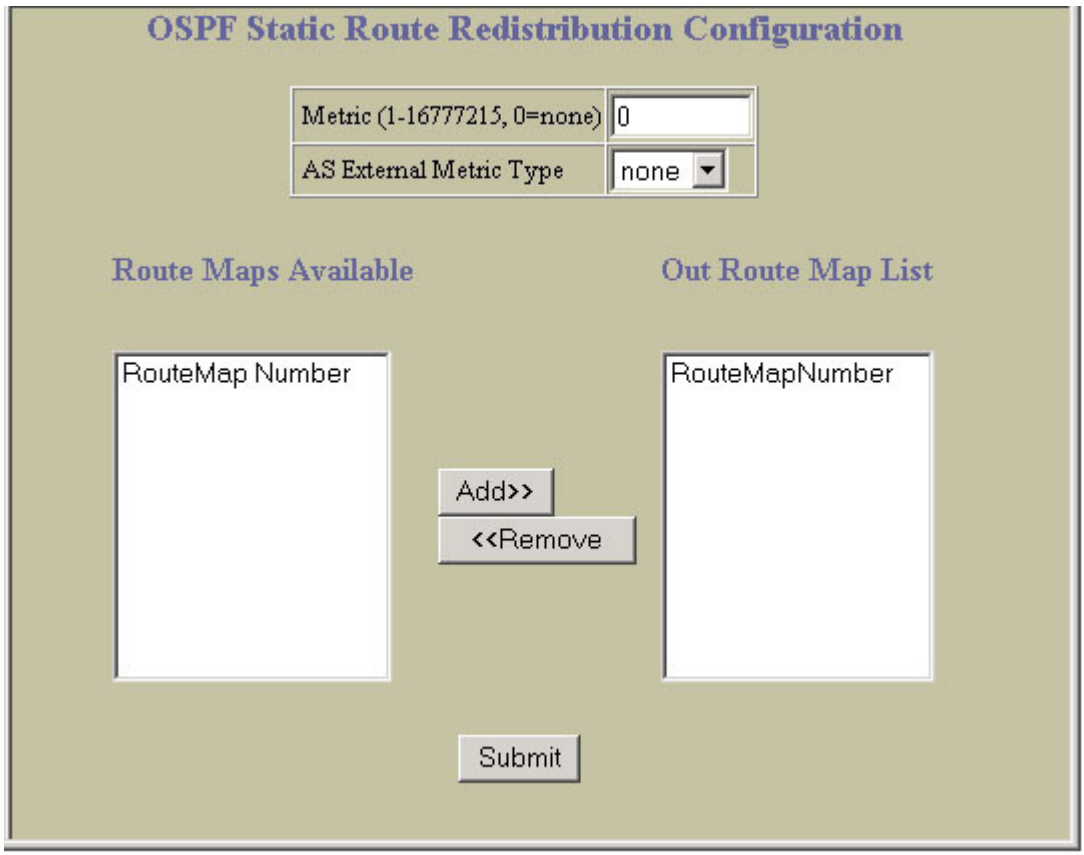
The following table describes the OSPF Host Configuration controls:

Table 157 OSPF Host Configuration controls

Control	Descriptions
Host Identifier (1-128)	Assigns a numeric identifier to the OSPF host.
IP Address	Defines the base IP address for the host entry.
Enabled?	Enables or disables the OSPF virtual link.
Area Number (0-2)	Defines the area index used by the OSPF host.
Output Cost (1-65535)	Defines the cost value of the host.

OSPF Route Redistribution Configuration

To display the following form, select **Layer 3 > OSPF Routing Protocol > OSPF Route Redistribution** (click the underlined text, not the folder).



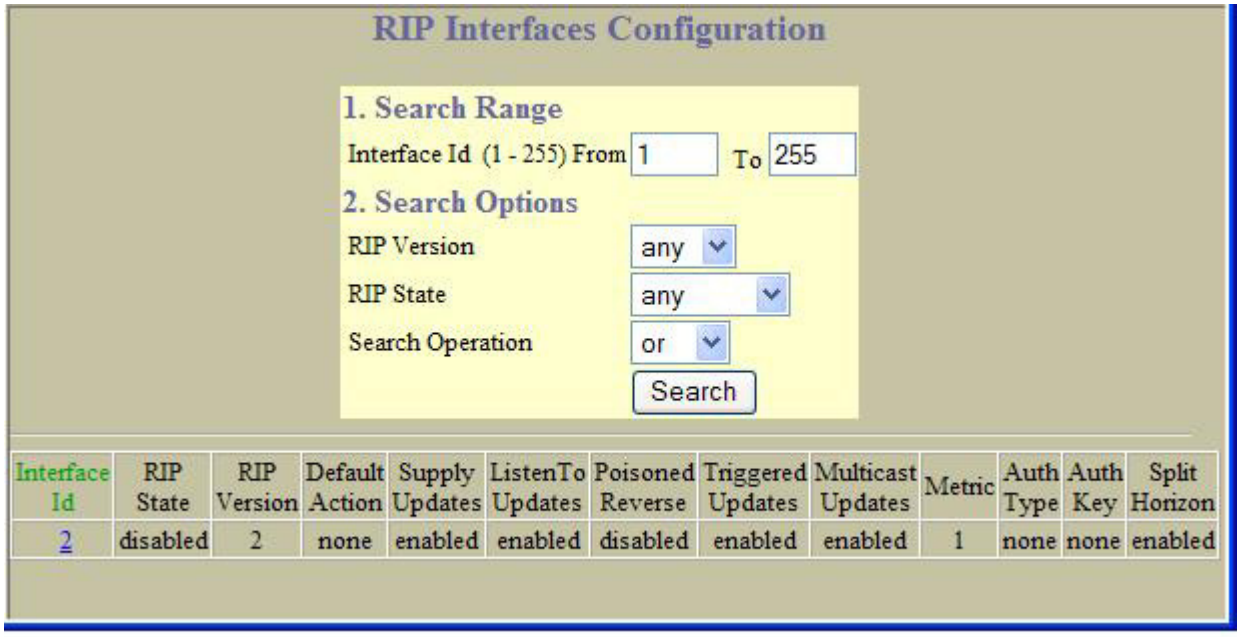
The following table describes the OSPF Route Redistribution Configuration controls:

Table 158 OSPF Route Redistribution Configuration controls

Control	Descriptions
Metric (1-16777215, 0=none)	Exports the routes of this protocol as external OSPF AS-external LSAs in which the metric and metric type are specified. To remove a previous configuration and stop exporting the routes of the protocol, enter `none`.
AS External Metric Type	Exports the routes of this protocol as external OSPF AS-external LSAs in which the metric and metric type are specified. To remove a previous configuration and stop exporting the routes of the protocol, enter `none`.
Route Maps Available	Lists the route maps that can be added to the list of OSPF static route.
Out Route Map List	Lists the route maps that are members of the OSPF static route. Select a route map number in the Route Maps Available list and click **Add** to add the route map to the list of static routes. Select a route map number in the Out Route Map list and click **Remove** to remove the route map from the list of static routes.

RIP Interfaces Configuration

To display the following form, select **Layer 3 > Routing Information Protocol > Routing Information Protocol** (click the underlined text, not the folder).



RIP is used for configuring Routing Information Protocol parameters. This option is turned off by default.

NOTE: Do not configure RIP1 parameters if your routing equipment uses RIP version 2.

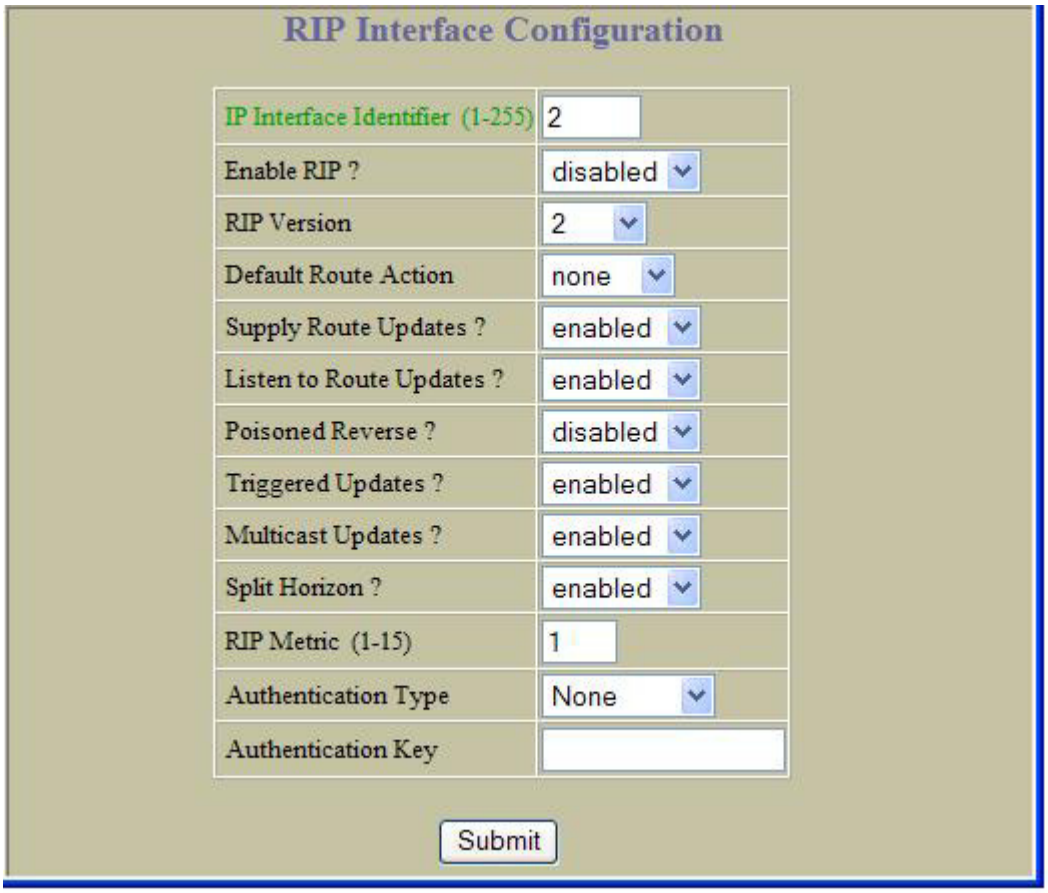
The following table describes the RIP Interfaces Configuration controls:

Table 159 RIP Interfaces Configuration controls

Control	Description
Search Range	To search for a RIP interface, enter a range of interface numbers in the **From** and **To** fields.
Search Options	To focus the search for a VLAN, enter optional search parameters: • RIP Version • RIP state Fields that have a value of "any" are ignored during the search. Choose a search operation: • **or**: Search for RIP interfaces specified in the search range that meet any of the criteria entered. • **and**: Search for RIP interfaces specified in the search range that meet all of the criteria entered. Click **Search** to display RIP interfaces that fit the range and meet the criteria entered.

RIP Interface Configuration

To display the following form, go to the RIP Interfaces Configuration form. Select a RIP interface number, or open the RIP Interfaces folder and click **Add RIP Interface**.



The following table describes the RIP Interface Configuration controls:

Table 160 RIP Interface Configuration controls

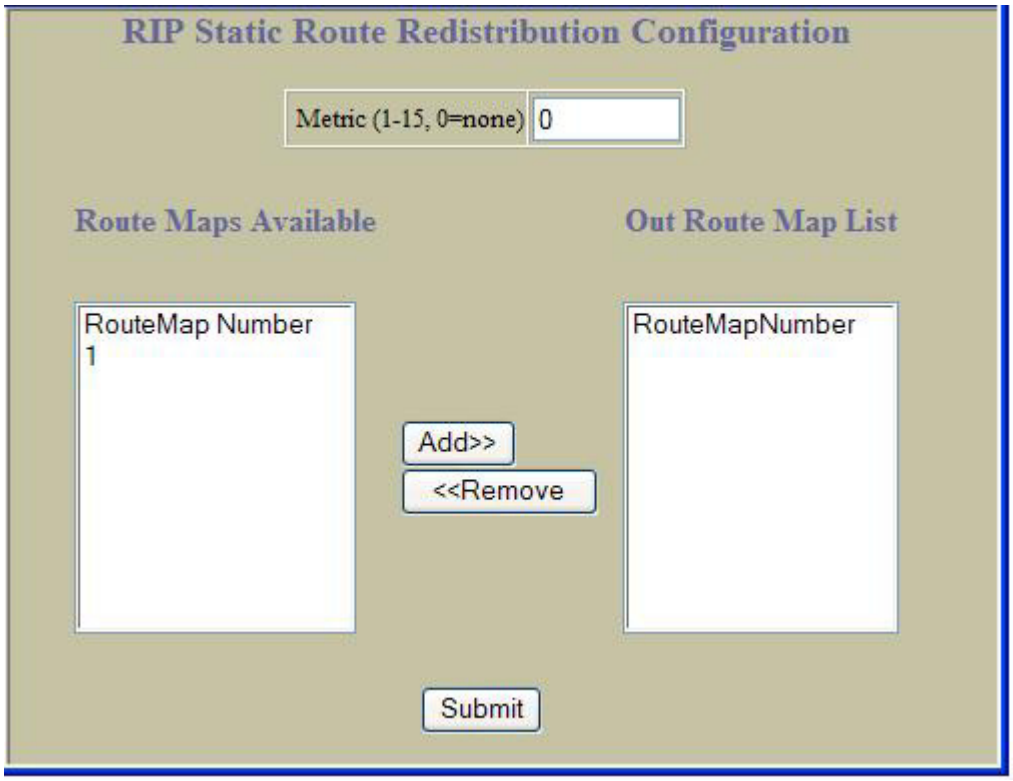
Control	Descriptions
IP Interface number (1-255)	Assigns a numeric identifier to the RIP interface.
Enable RIP?	Enables or disables the RIP interface.
RIP Version	Configures the RIP version used by this interface. The default value is **version 1**.
Default Route Action	When enabled, the switch accepts RIP default routes from other routers, but gives them lower priority than configured default gateways. When disabled, the switch rejects RIP default routes. The default value is **disabled**.
Supply Route Updates?	When enabled, the switch supplies routes to other routers. The default value is **disabled**.
Listen to Route Updates?	When enabled, the switch learns routes from other routers. The default value is **disabled**.
Poisoned Reverse?	When enabled, the switch uses split horizon with poisoned reverse. When disabled, the switch uses only split horizon. The default value is **disabled**.
Triggered Updates?	Enables or disables Triggered Updates. Triggered Updates are used to speed convergence. When enabled, Triggered Updates force a router to send update messages immediately, even if it is not yet time for the update message. The default value is **disabled**.
Multicast Updates?	Enables or disables multicast updates of the routing table (using address 224.0.0.9). The default value is **disabled**.
Split Horizon?	Enables or disables split horizon. The default value is **enabled**.

Table 160 RIP Interface Configuration controls

Control	Descriptions
RIP Metric (1-15)	Configures the route metric, which indicates the relative distance to the destination. The default value is **1**.
Authentication Type	Configures the authentication type. The default is `none`.
Authentication Key	Configures the authentication key password.

RIP Route Redistribution Configuration

To display the following form, select **Layer 3 > Routing Information Protocol > Static Route Redistribution, Fixed Route Redistribution, OSPF Route Redistribution,** or **OSPF External Route Redistribution**.



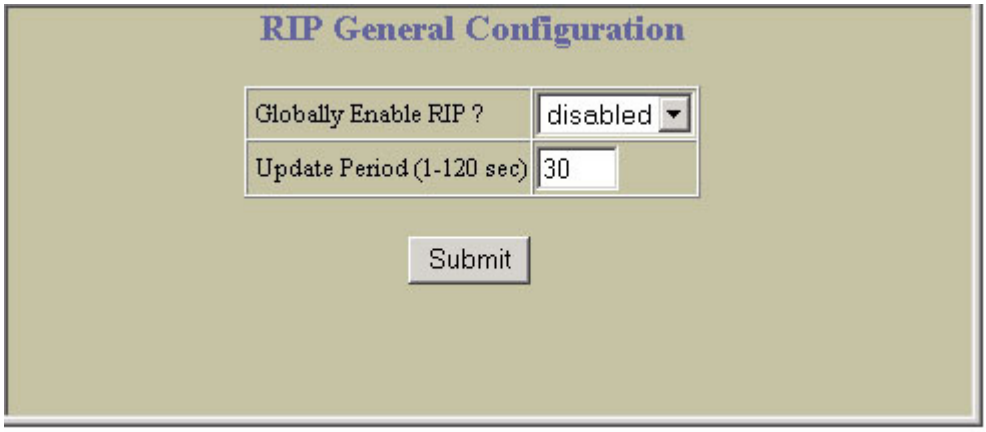
The following table describes the RIP Route Redistribution Configuration controls:

Table 161 RIP Route Redistribution Configuration controls

Control	Descriptions
Metric (1-15, 0 = none)	Exports the routes of this protocol in which the metric and metric type are specified. To remove a previous configuration and stop exporting the routes of the protocol, enter **0** (none).
Route Maps Available	Lists the route maps that can be added to the list of OSPF static route.
Out Route Map List	Lists the route maps that are members of the RIP route. Select a route map number in the Route Maps Available list and click **Add** to add the route map to the list of RIP Redistribution routes. Select a route map number in the Out Route Map list and click **Remove** to remove the route map from the list of RIP Redistribution routes.

RIP General Configuration

To display the following form, select **Layer 3 > Routing Information Protocol > General**.



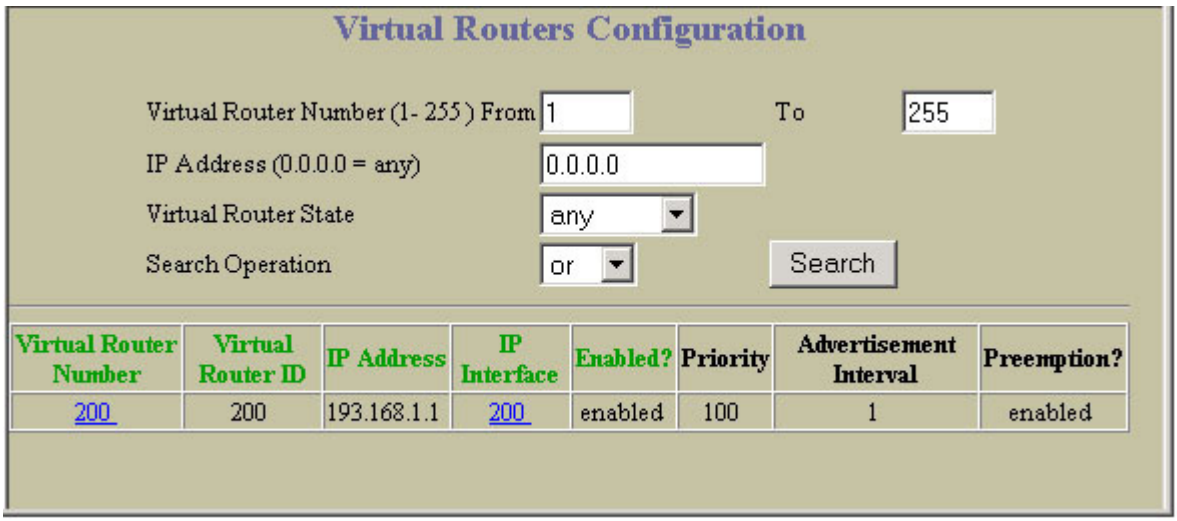
The following table describes the RIP Interface Configuration controls:

Table 162 RIP Interface Configuration controls

Control	Descriptions
Globally Enable RIP?	Globally enables or disables RIP.
Update Period (1-120 sec)	Configures the time interval for sending for RIP table updates, in seconds. The default value is 30 seconds.

Virtual Routers Configuration

To display the following form, select **Layer 3 > Virtual Router Redundancy Protocol > Virtual Routers** (click the underline text, not the folder).



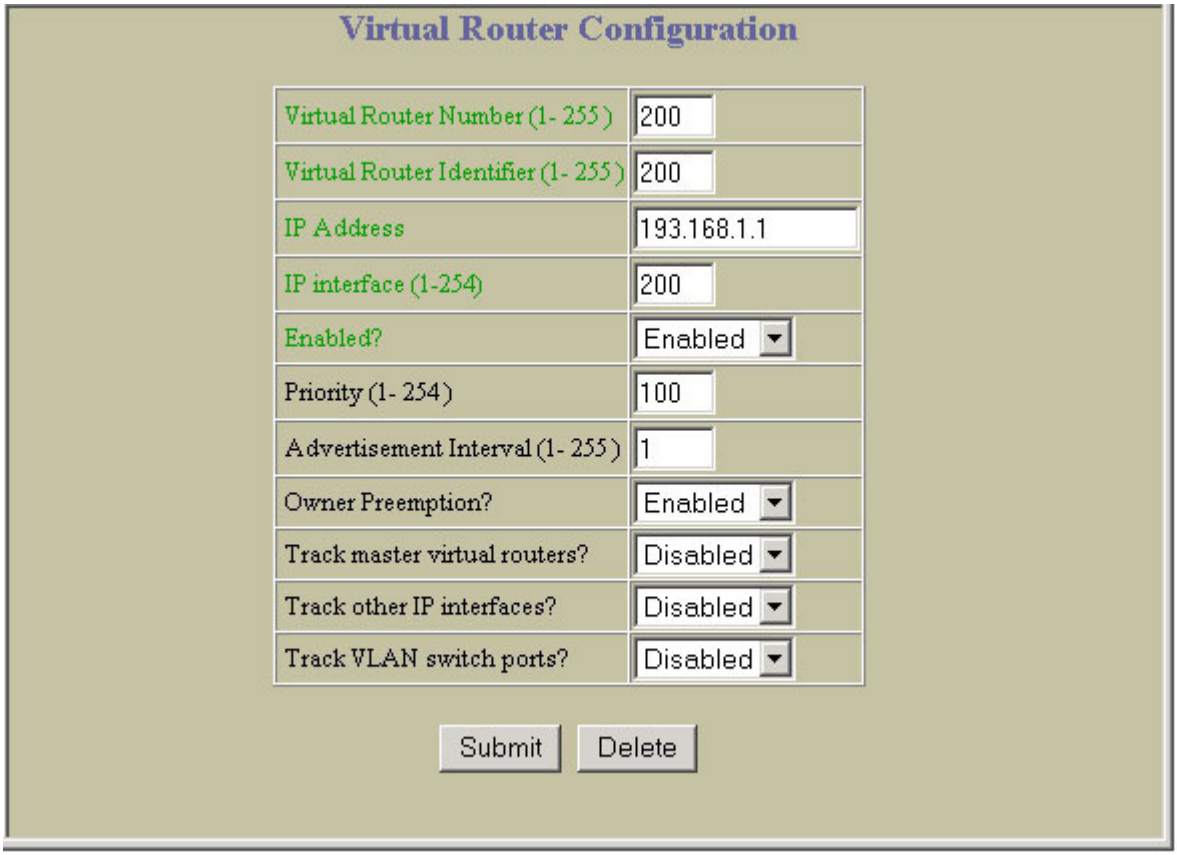
The following table describes Virtual Routers Configuration controls:

Table 163 Virtual Routers Configuration controls

Control	Description
Search Operation	To focus the search for an virtual router, enter search parameters: • Virtual Router number • IP Address • Virtual Router state Fields that have a value of "any" are ignored during the search. Choose a search operation: • **or**: Search for virtual routers specified in the Search range that meet any of the criteria entered. • **and**: Search for virtual routers specified in the Search range that meet all of the criteria entered. Click **Search** to display virtual routers that fit the range and meet the criteria entered.

Virtual Router Configuration

To display the following form, go to the Virtual Routers Configuration form. Select a Virtual Router number or open the Virtual Routers folder and click **Add Virtual Router**.



The following table describes the Virtual Router Configuration controls:

Table 164 Virtual Router Configuration controls

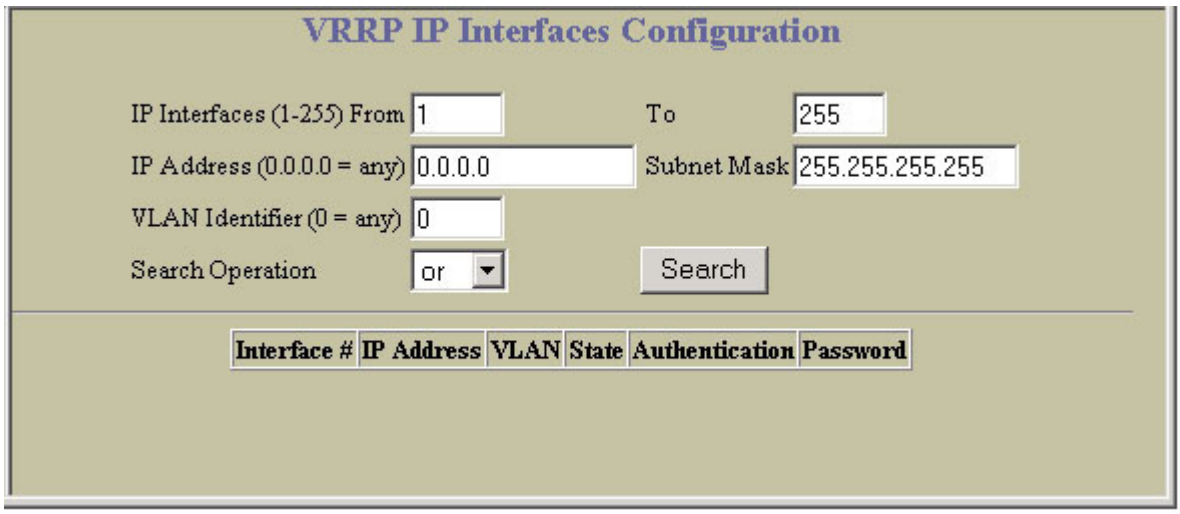
Control	Descriptions
Virtual Router Identifier (1-255)	Defines the virtual router ID. This is used in conjunction with `addr` (below) to define a virtual router on this switch. To create a pool of VRRP-enabled routing devices which can provide redundancy to each other, each participating VRRP device must be configured with the same virtual router: one that shares the same `vrid` and `addr` combination. The `vrid` for standard virtual routers (where the virtual router IP address is not the same as any virtual server) can be any integer between 1 and 255. The default value is 1. All `vrid` values must be unique within the VLAN to which the virtual router's IP interface belongs.

Table 164 Virtual Router Configuration controls

Control	Descriptions
IP Address	Defines the IP address for this virtual router using dotted decimal notation. This is used in conjunction with the `vrid` (above) to configure the same virtual router on each participating VRRP device. The default address is 0.0.0.0
IP Interface (1-255)	Selects a switch IP interface (between 1 and 255). If the IP interface has the same IP address as the `addr` option above, this switch is considered the "owner" of the defined virtual router. An owner has a special priority of 255 (highest) and will always assume the role of master router, even if it must preempt another virtual router which has assumed master routing authority. This preemption occurs even if the `preem` option below is disabled. The default value is 1.
Enabled?	Enables or disables this virtual router.
Priority (1-254)	Defines the election priority bias for this virtual server. This can be any integer between 1 and 254. The default value is 100. During the master router election process, the routing device with the highest virtual router priority number wins. If there is a tie, the device with the highest IP interface address wins. If this virtual router's IP address (`addr`) is the same as the one used by the IP interface, the priority for this virtual router will automatically be set to 255 (highest). When priority tracking is used (`/cfg/l3/vrrp/track` or `/cfg/l3/vrrp/vr #/track`), this base priority value can be modified according to a number of performance and operational criteria.
Advertisement Interval (1-255)	Defines the time interval between VRRP master advertisements. This can be any integer between 1 and 255 seconds. The default value is 1.
Owner Preemption?	Enables or disables master preemption. When enabled, if this virtual router is in backup mode but has a higher priority than the current master, this virtual router will preempt the lower priority master and assume control. Note that even when `preem` is disabled, this virtual router will always preempt any other master if this switch is the owner (the IP interface address and virtual router `addr` are the same). By default, this option is enabled.
Track master virtual routers?	When enabled, the priority for this virtual router will be increased for each virtual router in master mode on this switch. This is useful for making sure that traffic for any particular client/server pairing are handled by the same switch, increasing routing and load balancing efficiency. This command is disabled by default.
Track other IP interfaces?	When enabled, the priority for this virtual router will be increased for each other IP interface active on this switch. An IP interface is considered active when there is at least one active port on the same VLAN. This helps elect the virtual routers with the most available routes as the master. This command is disabled by default.
Track VLAN switch ports?	When enabled, the priority for this virtual router will be increased for each active port on the same VLAN. A port is considered "active" if it has a link and is forwarding traffic. This helps elect the virtual routers with the most available ports as the master. This command is disabled by default.

VRRP Interfaces Configuration

To display the following form, select **Layer 3 > Virtual Router Redundancy Protocol > VRRP Interfaces** (click the underline text, not the folder).



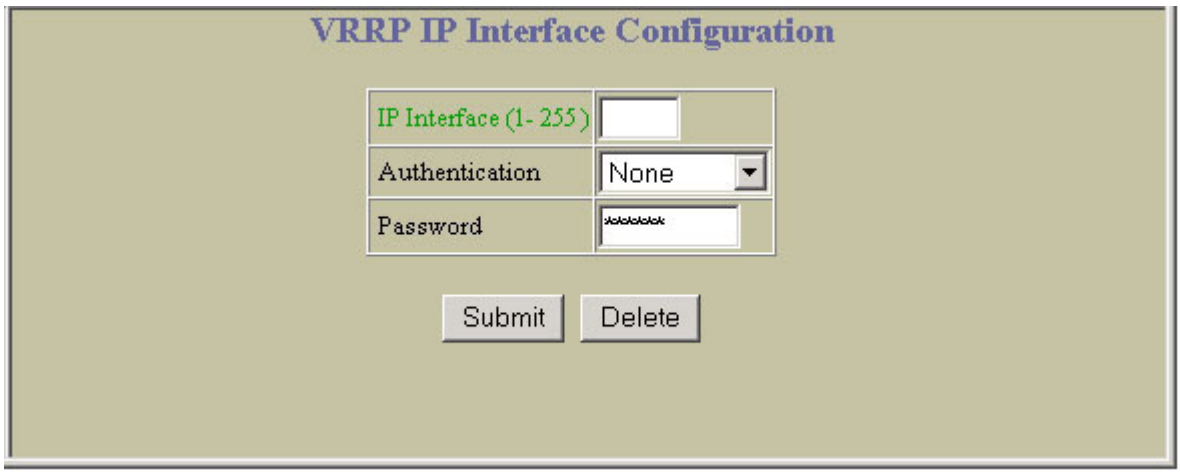
The following table describes VRRP Interfaces Configuration controls:

Table 165 VRRP Interfaces Configuration controls

Control	Description
Search Operation	To focus the search for an virtual router, enter search parameters: • IP Interfaces • IP Address and subnet mask • VLAN ID Fields that have a value of "any" are ignored during the search. Choose a search operation: • **or**: Search for VRRP interfaces specified in the Search range that meet any of the criteria entered. • **and**: Search for VRRP interfaces specified in the Search range that meet all of the criteria entered. Click **Search** to display VRRP interfaces that fit the range and meet the criteria entered.

VRRP Interface Configuration

To display the following form, go to the Virtual Routers Configuration form. Select a VRRP interface number or open the VRRP Interfaces folder and click **Add Virtual router Interface**.



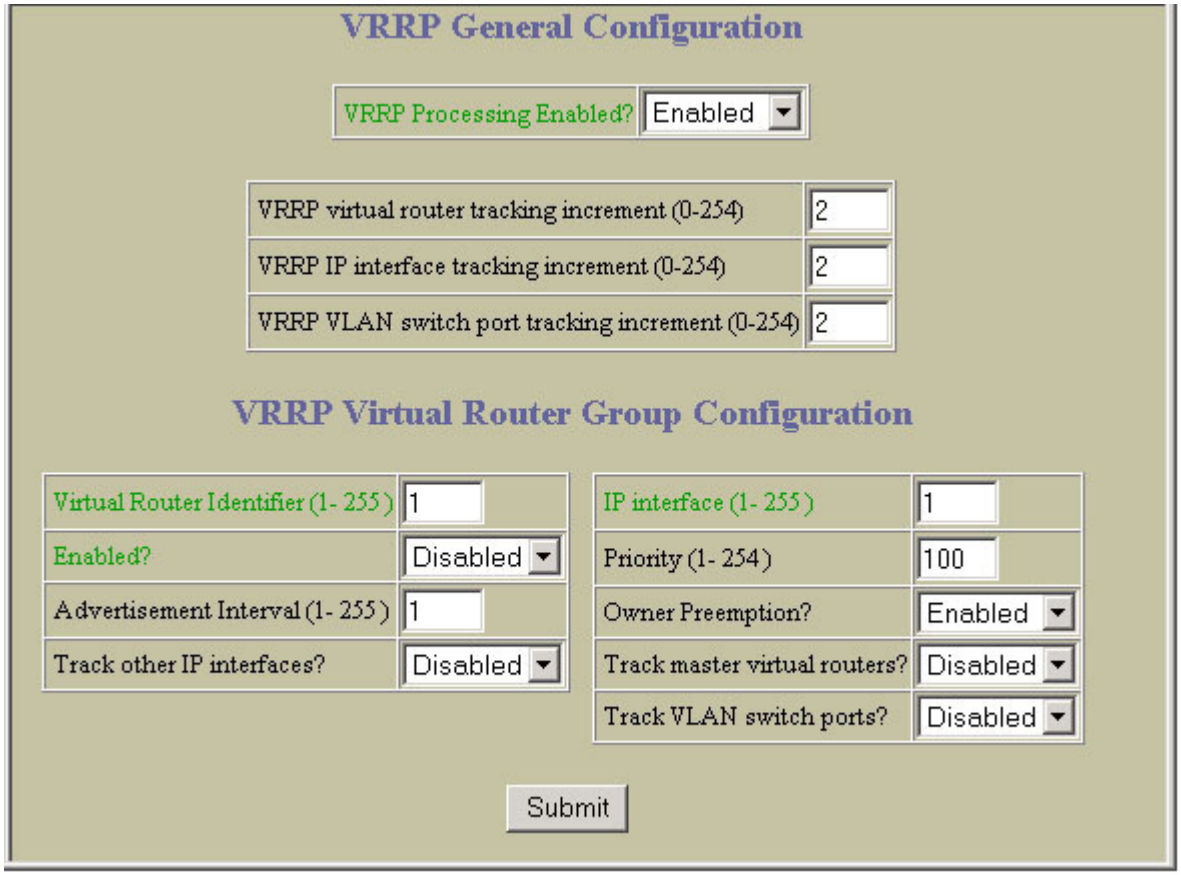
The following table describes the VRRP Interface Configuration controls:

Table 166 VRRP Interface Configuration controls

Control	Descriptions
IP Interface (1-255)	Defines the IP interface.
Authentication?	Defines the type of authentication that will be used: `none` (no authentication), or `password` (password authentication).
Password	Defines a plain text password up to eight characters long. This password will be added to each VRRP packet transmitted by this interface when password authentication is chosen (see **`Authentication`** above).

VRRP General Configuration

To display the following form, select **Layer 3 > Virtual Router Redundancy Protocol > General.**



The following table describes the VRRP General Configuration controls:

Table 167 VRRP General Configuration controls

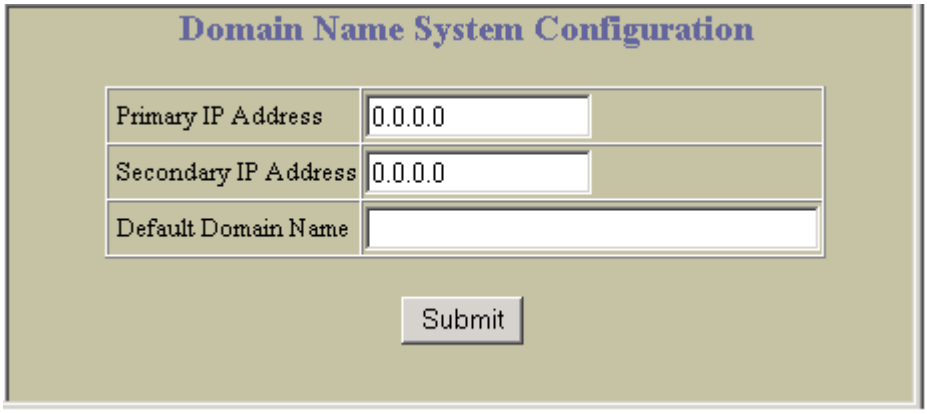
Control	Descriptions
VRRP Processing Enabled?	Globally enables or disables VRRP processing.
VRRP virtual router tracking increment (0-254)	Defines the priority increment value (1 through 254) for virtual routers in master mode detected on this switch. The default value is 2.
VRRP IP interface tracking increment (0-254)	Defines the priority increment value (1 through 254) for active IP interfaces detected on this switch. The default value is 2.
VRRP VLAN switch port tracking increment (0-254)	Defines the priority increment value (1 through 254) for active ports on the virtual router's VLAN. The default value is 2.
VRRP Virtual Router Group Configuration	
Virtual Router Identifier (1-255)	Assigns a numeric identifier to the virtual router group.

Table 167 VRRP General Configuration controls

Control	Descriptions
IP interface (1-255)	Defines the IP interface associated with the virtual router group.
Enabled?	Enables or disables the virtual router group.
Priority (1-254)	Defines the election priority bias for this virtual router group. This can be any integer between 1 and 254. The default value is 100. During the master router election process, the routing device with the highest virtual router priority number wins. If there is a tie, the device with the highest IP interface address wins. If this virtual router's IP address (`addr`) is the same as the one used by the IP interface, the priority for this virtual router will automatically be set to 255 (highest). When priority tracking is used (`/cfg/l3/vrrp/track` or `/cfg/l3/vrrp/vr #/track`), this base priority value can be modified according to a number of performance and operational criteria.
Advertisement Interval (1-255)	Defines the time interval between VRRP master advertisements. This can be any integer between 1 and 255 seconds. The default is 1.
Owner Preemption?	Enables or disables master preemption. When enabled, if the virtual router group is in backup mode but has a higher priority than the current master, this virtual router will preempt the lower priority master and assume control. Note that even when `preem` is disabled, this virtual router will always preempt any other master if this switch is the owner (the IP interface address and virtual router `addr` are the same). By default, this option is enabled.
Track other IP interface?	When enabled, the priority for this virtual router will be increased for each other IP interface active on this switch. An IP interface is considered active when there is at least one active port on the same VLAN. This helps elect the virtual routers with the most available routes as the master. This command is disabled by default.
Track master virtual routers?	When enabled, the priority for this virtual router will be increased for each virtual router in master mode on this switch. This is useful for making sure that traffic for any particular client/server pairing are handled by the same switch, increasing routing and load balancing efficiency. This command is disabled by default.
Track VLAN switch ports?	When enabled, the priority for this virtual router will be increased for each active port on the same VLAN. A port is considered "active" if it has a link and is forwarding traffic. This helps elect the virtual routers with the most available ports as the master. This command is disabled by default.

Domain Name System Configuration

To display the following form, select **Layer 3 > Domain Name System**.



The Domain Name System (DNS) Menu is used for defining the primary and secondary DNS servers on your local network, and for setting the default domain name served by the switch services. DNS parameters must be configured prior to using hostname parameters with the `ping`, `traceroute`, and `tftp` commands.

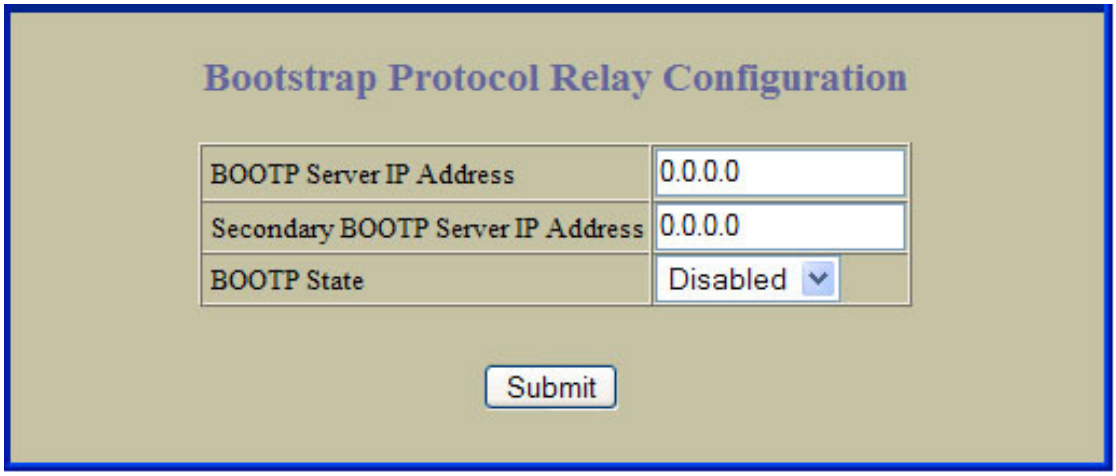
The following table describes the Domain Name System Configuration controls:

Table 168 Domain Name System Configuration controls

Control	Description
Primary IP Address	Sets the IP address for your primary DNS server. Use dotted decimal notation.
Secondary IP Address	Sets the IP address for your secondary DNS server. If the primary DNS server fails, the configured secondary will be used instead. Enter the IP address using dotted decimal notation.
Default Domain Name	Sets the default domain name used by the switch. For example: `mycompany.com`.

Bootstrap Protocol Relay Configuration

To display the following form, select **Layer 3 > Bootstrap Protocol Relay**.



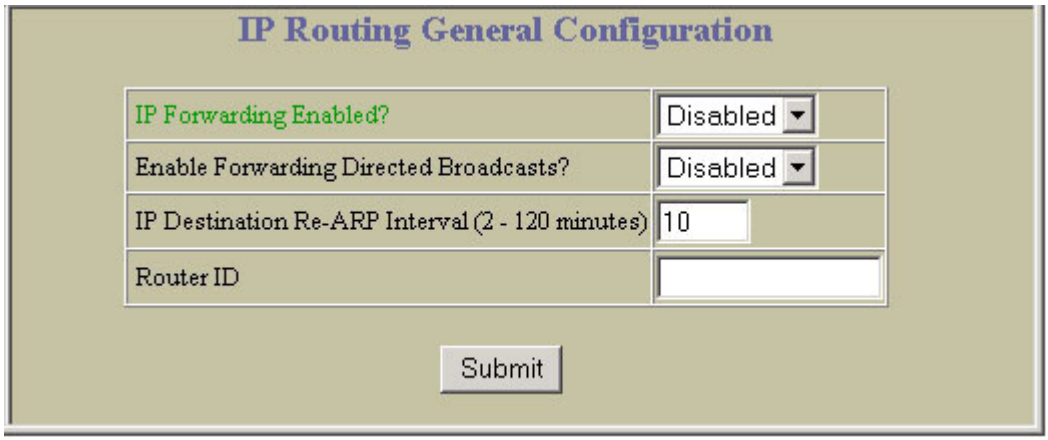
The following table describes the Bootstrap Protocol Relay configuration controls:

Table 169 Bootstrap Protocol Relay Configuration controls

Control	Description
BOOTP Server IP Address	Sets the IP address of the BOOTP server.
Secondary BOOTP Server IP Address	Sets the IP address of the secondary BOOTP server.
BOOTP State	Enables or disables the use of BOOTP. If you enable BOOTP, the GbE2 Interconnect Switch will query its BOOTP server for all of the GbE2 Interconnect Switch IP parameters. The default is **enable**.

IP Routing General Configuration

To display the following form, select **Layer 3 > General**.



The following table describes the IP Routing General Configuration controls:

Table 170 IP Routing General Configuration controls

Control	Description
IP Forwarding Enabled?	Enables or disables IP Forwarding.
Enable Forwarding Directed Broadcasts?	Enables or disables forwarding directed broadcasts.
IP Destination Re-ARP Interval (2-120 minutes)	Sets the re-ARP period in minutes. The switch periodically sends ARP (Address Resolution Protocol) requests to refresh its address database. This command is used for setting the interval between ARP refreshes of the next IP address in the database. The default interval is 10 minutes.
Router ID	Configures the router ID.

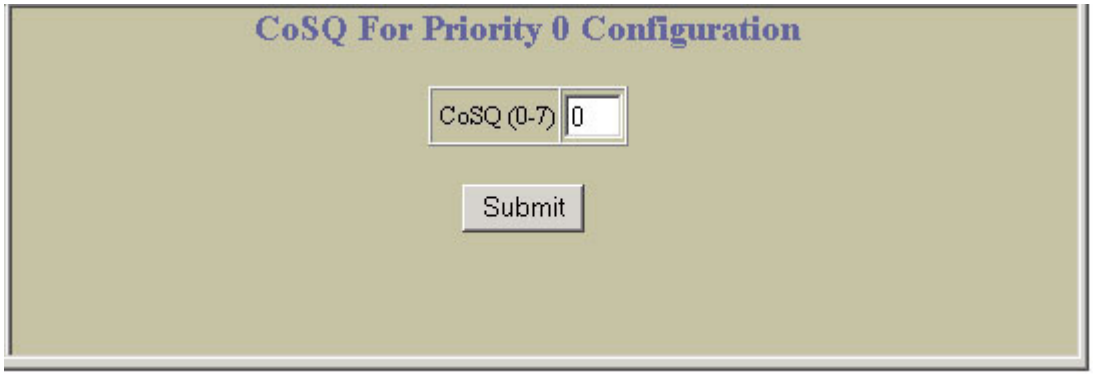
QoS Priority CoS Configuration

To display the following form, select **QoS > 802.1p > Priority - CoS**.

This form summarizes the QoS Priority – Class of Service parameters. Select a priority value to view the CoSQ For Priority form.

QoS Priority CoS Queue Configuration

To display the following form, go to the Priority – CoS form, and select a priority value.



The following table describes the CoSQ For Priority configuration controls:

Table 171 CoSQ For Priority Configuration controls

Control	Description
CoSQ (0-7)	Maps the 802.1p priority of to the Class of Service queue (CoSq) priority. Enter the Class of Service queue (0-7) that handles the matching traffic.

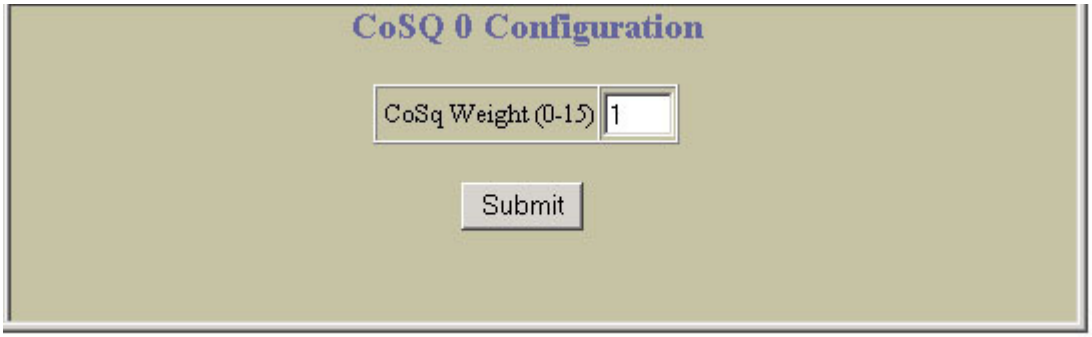
QoS CoS Weight Configuration

To display the following form, select **QoS > 802.1p > CoS - Weight**.

This form summarizes the QoS Class of Service Weight parameters. Select a Class of Service (CoS) value to view the form.

QoS CoS Queue Configuration

To display the following form, go to the CoS –Weight Configuration form, and select a CoS value.



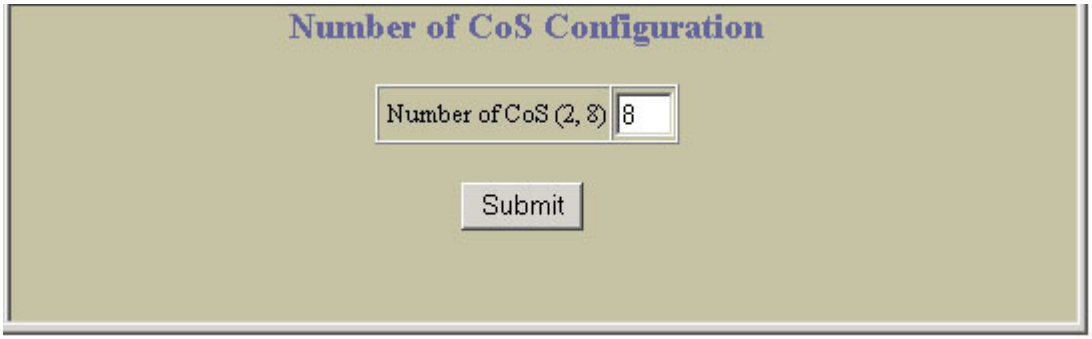
The following table describes the CosQ configuration controls:

Table 172 CoSQ Configuration controls

Control	Description
CoSq Weight (0-15)	Configures the scheduling weight of the selected Class of Service queue (CoSq).

QoS Number of CoS Configuration

To display the following form, select **QoS > 802.1p > Number of CoS**.



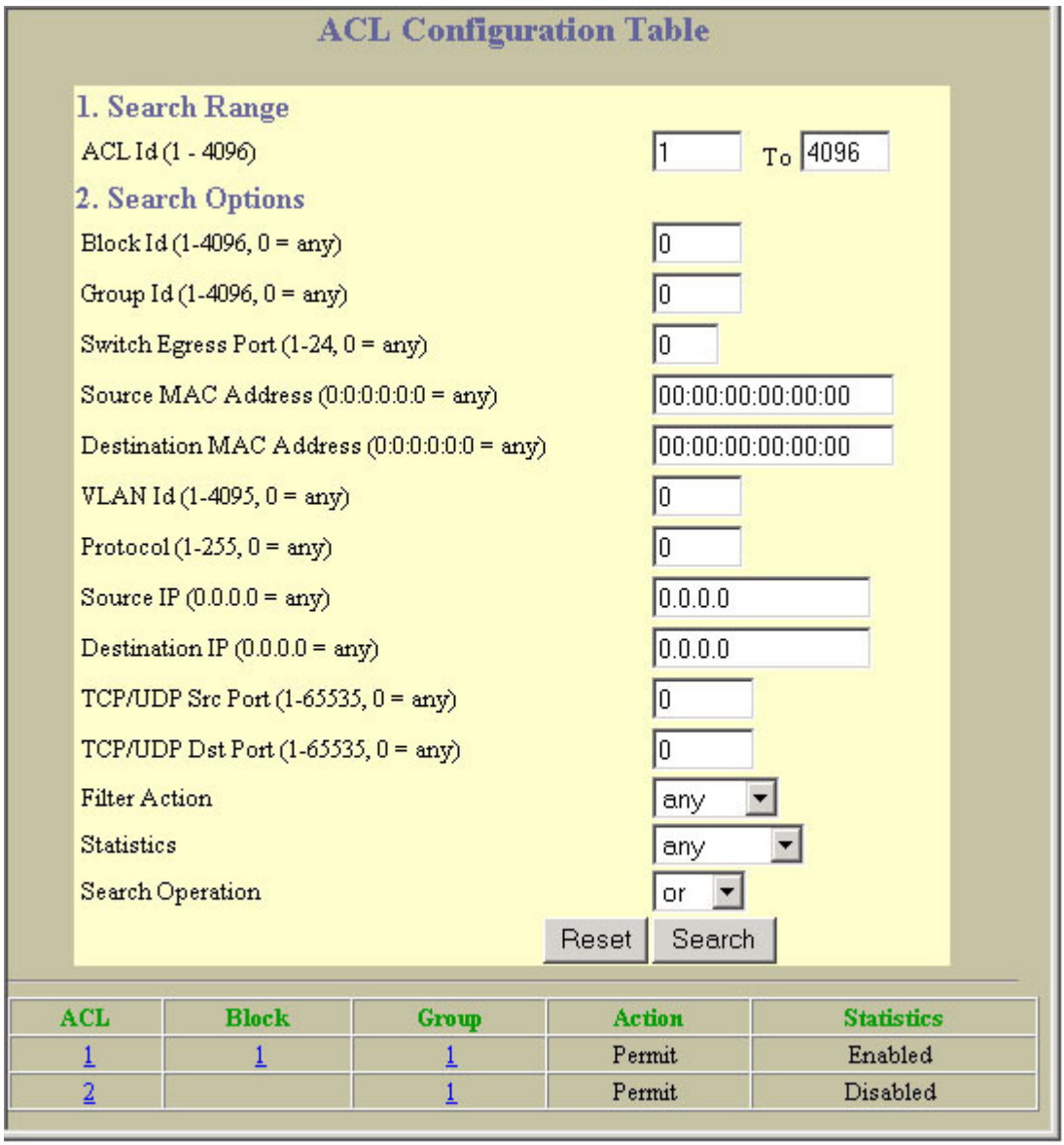
The following table describes the CosQ configuration controls:

Table 173 Number of CoSQ Configuration controls

Control	Description
Number of CoSq (2, 8)	Sets the number of Class of Service queues for switch ports. Default is 8.

ACL Configuration

To display the following form, select **Access Control > Access Control Lists** (click the underlined text, not the folder).



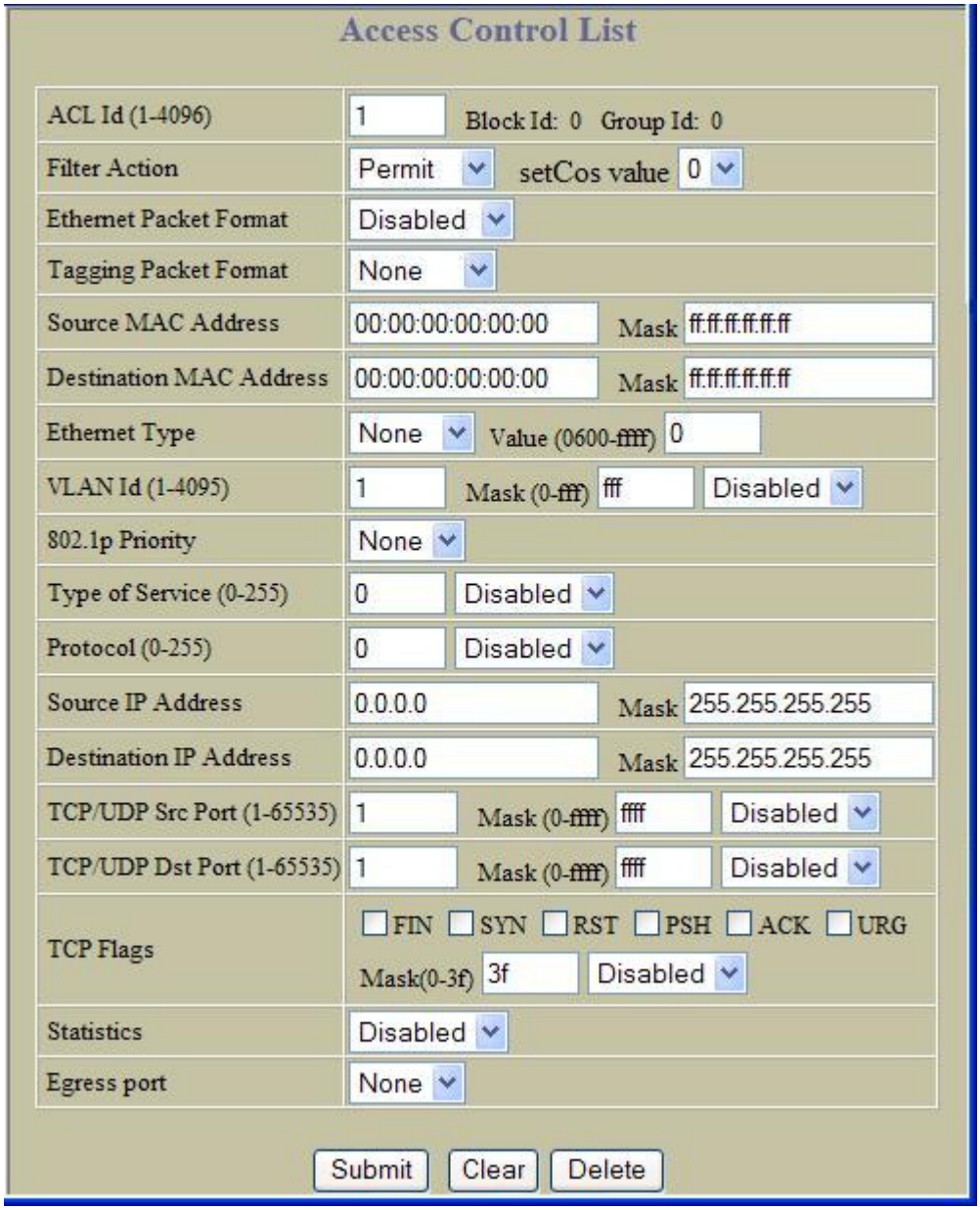
This form allows you to search for Access Control Lists. The following table describes the ACL Configuration controls:

Table 174 ACL Configuration controls

Control	Description
Search Range	To search for an ACL, enter a range of ACL ID numbers in the **From** and **To** fields.
Search Options	To focus the search for an ACL, enter optional search parameters: • Block ID • Group ID • Switch Egress Port • Source MAC address • Destination MAC address • VLAN ID • Protocol type • Source IP address • Destination IP address • TCP/UDP source port • TCP/UDP destination port • Filter action • Statistics Fields that have a value of "any" are ignored during the search. Choose a search operation: • **or**: Search for ACLs specified in the search range that meet any of the criteria entered. • **and**: Search for ACLs specified in the search range that meet all of the criteria entered. Click **Search** to display ACLs that fit the range and meet the criteria entered.

Access Control List Configuration

To display the following form, go to the ACL Configuration Table form, and select an ACL number.



This form allows you to define filtering criteria for the Access Control List (ACL).The following table describes the Access Control List configuration controls:

Table 175 Access Control List Configuration controls

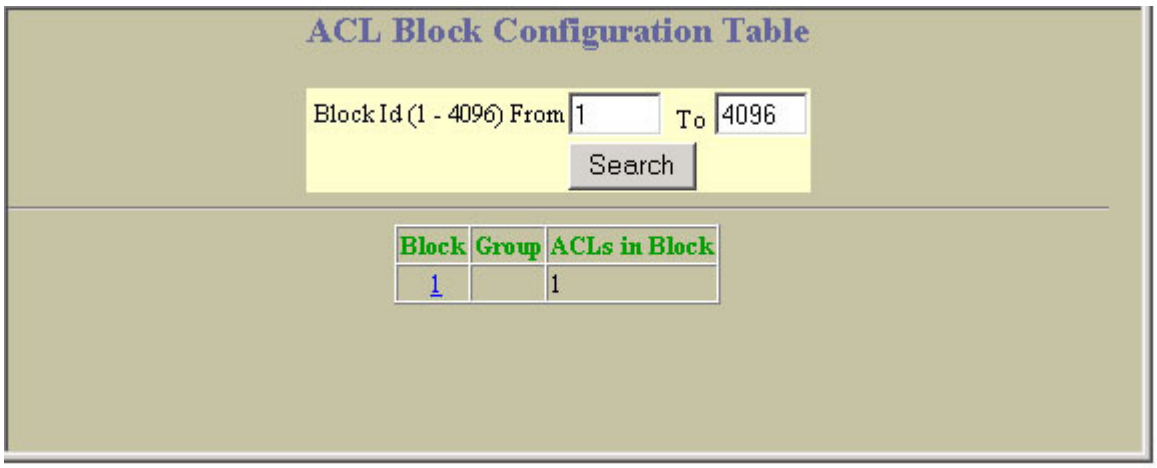
Control	Description
ACL ID (1-4096)	Assigns a numeric identifier to the ACL.
Filter Action	Configures a filter action for packets that match the ACL definitions. You can choose to permit (pass) or deny (drop) packets, or set the Class of Service queue that handles the packets.
Ethernet Packet Format	Defines the Ethernet format for the ACL.
Tagging Packet Format	Defines the tagging format for the ACL.
Source MAC Address	Defines the source MAC address for this ACL.
Destination MAC Address	Defines the destination MAC address for this ACL.
Ethernet Type	Defines the Ethernet type for this ACL.

Table 175 Access Control List Configuration controls

Control	Description
VLAN ID (1-4095)	Defines a VLAN number and mask for this ACL.
802.1p Priority	Defines the 802.1p priority for the ACL.
Type of Service (0-255)	Defines a Type of Service value for the ACL. For more information on ToS, see RFC 1340 and 1349.
Protocol (0-255)	Defines an IP protocol for the ACL. If defined, traffic from the specified protocol matches this filter. Specify the protocol number. Listed below are some of the well-known protocols. **Number** **Name** 1 icmp 2 igmp 6 tcp 17 udp 89 ospf 112 vrrp
Source IP Address	Defines a source IP address for the ACL. If defined, traffic with this source IP address will match this ACL. Specify an IP address in dotted decimal notation.
Destination IP Address	Defines a destination IP address for the ACL. If defined, traffic with this destination IP address will match this ACL.
TCP/UDP Src Port (1-65535)	Defines a source port for the ACL. If defined, traffic with the specified TCP or UDP source port will match this ACL. Specify the port number. Listed below are some of the well-known ports: **Number** **Name** **20** ftp-data **21** ftp **22** ssh **23** telnet **25** smtp **37** time **42** name **43** whois **53** domain **69** tftp **70** gopher **79** finger **80** http
TCP/UDP Dst Port (1-65535)	Defines a destination port for the ACL. If defined, traffic with the specified TCP or UDP destination port will match this ACL. Specify the port number, just as with `sport` above.
TCP Flags	Defines a TCP/UDP flag for the ACL.
Statistics	Enables or disables the statistics collection for the ACL.
Egress Port	Selects an egress port to add to the ACL.

ACL Block Configuration

To display the following form, select **Access Control > Access Control Blocks** (click the underlined text, not the folder).



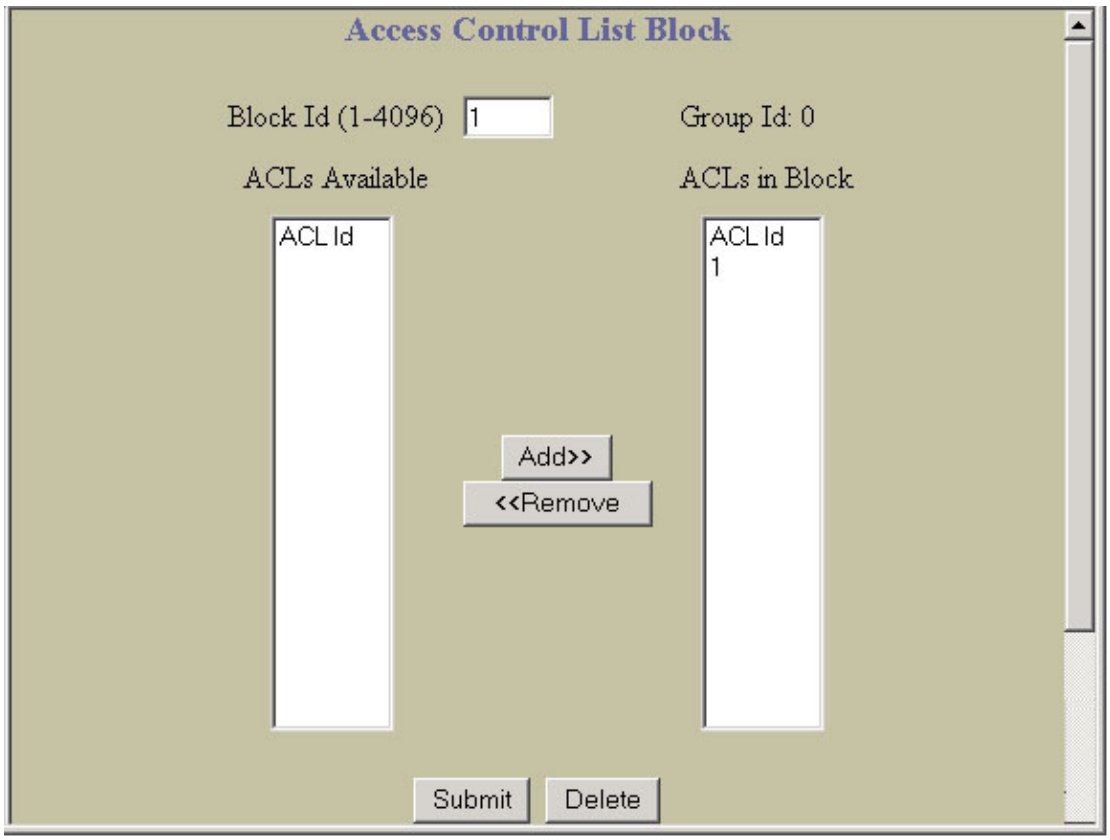
The following table describes the ACL Block Configuration controls:

Table 176 ACL Block Configuration controls

Control	Description
Search Range	To search for an ACL Block, enter a range of ACL Block numbers in the **From** and **To** fields. Click **Search** to display ACL Blocks that fit the range.

Access Control Block Configuration

To display the following form, go to the ACL Blocks Configuration Table form, and select an ACL Block number.



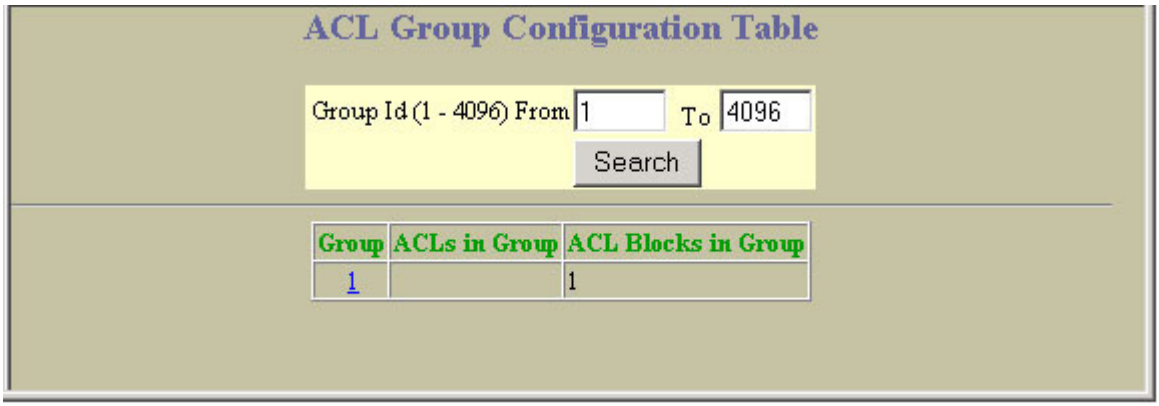
The following table describes the Access Control List Block configuration controls:

Table 177 Access Control List Block Configuration controls

Control	Description
Block ID (1-4096)	Assigns a numeric identifier to the ACL Block.
Group ID	Displays the Group ID for this ACL Block, if available.
ACLs Available	Lists the ACLs that you can add to the ACL Block.
ACLs in Block	Lists the ACLs that belong to the ACL Block. Select an ACL number in the ACLs Available list, and click **Add** to add the ACL to the ACL Block. Select an ACL number in the ACLs in Block list, and click **Remove** to remove the ACL from the ACL Block.

ACL Groups Configuration

To display the following form, select **Access Control > Access Control Groups** (click the underlined text, not the folder).



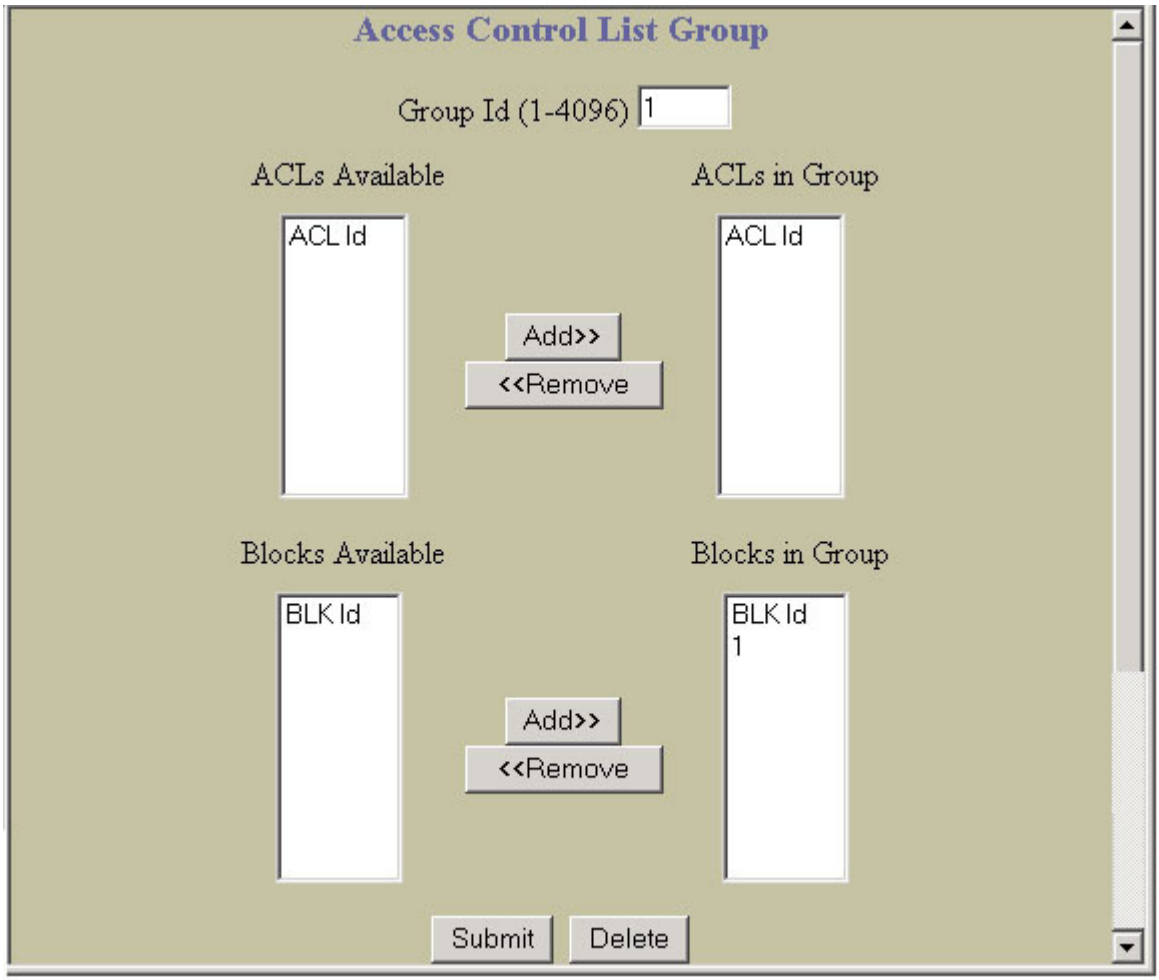
The following table describes the ACL Groups Configuration controls:

Table 178 ACL Groups Configuration controls

Control	Description
Search Range	To search for an ACL Group, enter a range of ACL Group numbers in the **From** and **To** fields. Click **Search** to display ACL Groups that fit the range.

Access Control Group Configuration

To display the following form, go to the ACL Groups Configuration Table form, and select an ACL Group number.



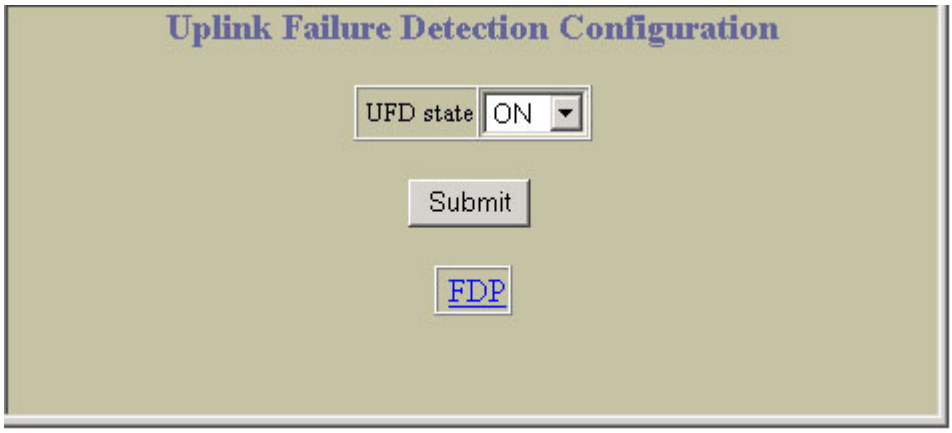
The following table describes the Access Control List Group configuration controls:

Table 179 Access Control List Group Configuration controls

Control	Description
Group ID (1-4096)	Assigns a numeric identifier to the ACL Group.
ACLs Available	Lists the ACLs that you can add to the ACL Group.
ACLs in Group	Lists the ACLs that belong to the ACL Group. Select an ACL number in the ACLs Available list, and click **Add** to add the ACL to the ACL Group. Select an ACL number in the ACLs in Group list, and click **Remove** to remove the ACL from the ACL Group.
Blocks Available	Lists the ACL Blocks that you can add to the ACL Group.
Blocks in Group	Lists the ACL Blocks that belong to the ACL Group. Select an ACL Block number in the Blocks Available list, and click **Add** to add the ACL Block to the ACL Group. Select an ACL Block number in the Blocks in Group list, and click **Remove** to remove the ACL Block from the ACL Group.

Uplink Failure Detection Configuration

To display the following form, select **Uplink Failure Detection** (click the underlined text, not the folder).



Uplink Failure Detection (UFD) supports network fault tolerance in network adapter teams. Use this menu to configure a Failure Detection Pair of one Links to Monitor (LtM) group and one Links to Disable (LtD) group. When UFD is enabled and a Failover Pair is configured, the switch automatically disables ports in the LtD if it detects a failure in the LtM. The failure conditions which are monitored in the LtM group include port link state moving to down, or port state moving to Blocking if Spanning Tree Protocol is enabled.

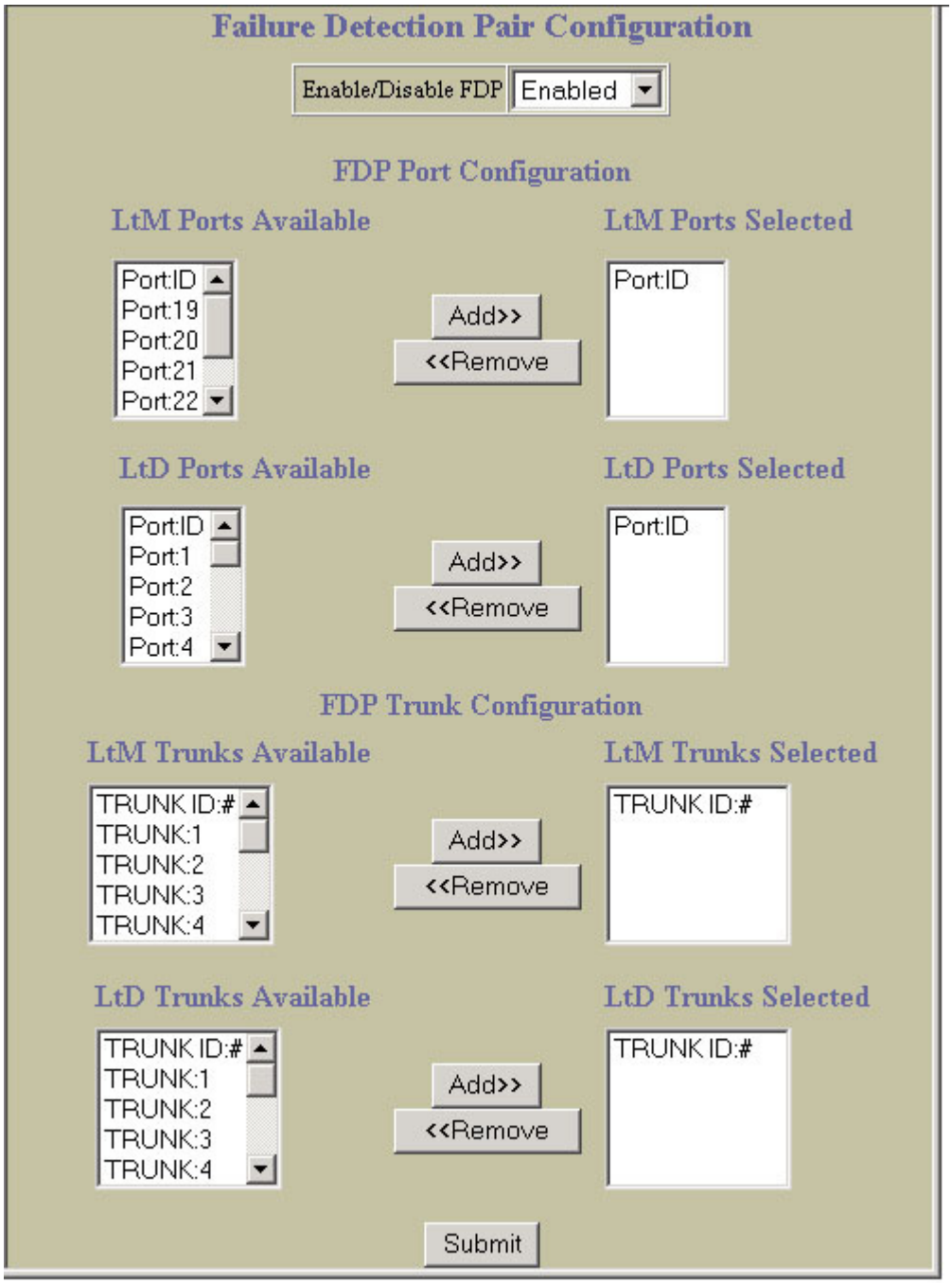
The following table describes the Uplink Failure Detection (UFD) configuration controls:

Table 180 Uplink Failure Detection Configuration controls

Control	Description
UFD state	Globally turns UFD **on** or **off**.
FDP	Displays the Failure Detection Pair Configuration form.

Failure Detection Pair Configuration

To display the following form, select **Uplink Failure Detection** (click the underlined text, not the folder). On the UFD Configuration form, select **FDP**.



The following table describes the Failure Detection Pair Configuration controls:

Table 181 Failure Detection Pair Configuration controls

Control	Description
Enable/Disable FDP	Enables or disables the Failover Pair.
LtM Ports Available	Lists the ports that can be added to the Link to Monitor (LtM). Only uplink ports (19-24) are allowed in the LtM.
LtM Ports Selected	Lists the ports that are members of the LtM. Select a port number in the LtM Ports Available list and click **Add** to add the port to the LtM. Select a port number in the LtM Ports Selected list and click **Remove** to remove the port from the LtM.
LtD Ports Available	Lists the ports that can be added to the Link to Disable (LtD). Only downlink ports (1-16) are allowed in the LtD.
LtD Ports Selected	Lists the ports that are members of the LtD. Select a port number in the LtD Ports Available list and click **Add** to add the port to the LtD. Select a port number in the LtD Ports Selected list and click **Remove** to remove the port from the LtD.
LtM Trunks Available	Lists the trunk groups that can be added to the Link to Monitor (LtM). The LtM trunk group can contain only uplink ports (19-24).
LtM Trunks Selected	Lists the trunk groups that are members of the LtM. Select a trunk group number in the LtM Trunks Available list and click **Add** to add the trunk group to the LtM. Select a trunk group number in the LtM Trunks Selected list and click **Remove** to remove the trunk group from the LtM.
LtD Trunks Available	Lists the trunk groups that can be added to the Link to Disable (LtD). LtD trunk groups can contain only downlink ports (1-16).
LtD Trunks Selected	Lists the trunk groups that are members of the LtD. Select a trunk group number in the LtD Trunks Available list and click **Add** to add the trunk group to the LtD. Select a trunk group number in the LtD Trunks Selected list and click **Remove** to remove the trunk group from the LtD.